Technical Support Working Group

2004 TSWG REVIEW

ANTITERRORISM

COUNTERTERRORISM

INTELLIGENCE SUPPORT

CONSEQUENCE MANAGEMENT

COMBATING TERRORISM

"Led by the United States, nations all around the globe have come together in an historic effort to wipe terrorism from the face of the Earth. Faithful friends and former foes alike have united against terror, and we are bringing every tool of statecraft to bear against it – military, intelligence, law enforcement, financial, and most certainly diplomatic."

Secretary of State Colin L. Powell, September 11, 2003

The Global War on Terrorism (GWOT) demands that the tools of statecraft operate on a foundation of technologies that can better protect us and more effectively defeat our enemies. Our competitive advantage against ruthless, determined, and intelligent terrorist adversaries depends critically upon the steady development and deployment of technologies that meet the specific requirements of armed forces, first responders, intelligence operatives, and diplomats. Technology underlies our ability to detect and identify threats in advance through superior intelligence gathering and interpreting techniques.

Technologies allow us to protect our seaports, airports, and border crossings as we improve the security of our complex, intermodal transportation systems and other critical infrastructure. Technologies are essential to detect and defeat the conventional and improvised explosives that terrorists and insurgents are using against innocent civilians and military personnel. The advancement and implementation of such technologies offer better ways to protect citizens of all nations.

Success in the GWOT will depend upon a determined mobilization of virtually every sector of our society. As Deputy Secretary of State Richard L. Armitage noted recently,[1]

"We must be prepared to take a stand because it is not just the magnificence of our military…that truly distinguishes America. Nor is it the might of our economy; and the appeal of our culture. It is the rule of law, and the equal right to opportunity. It is the freedom of mind and spirit and voice; and the energy and optimism of the American character."

The attributes of mind, spirit, and character to which Deputy Secretary Armitage refers are reflected in the cornucopia of technologies that have been realized through the creative genius of scientists and engineers from the United States and around the world.

The Technical Support Working Group (TSWG) has led the development of combating terrorism technologies since 1986. It has done so in a unique interagency forum that was created to cross traditional bureaucratic lines in order to define user-based counterterrorism technology requirements across the entire Federal establishment. This interagency cooperative body has mobilized the creativity of industry, academic institutions, private companies, and national laboratories to secure solutions to the most urgent technical requirements in the GWOT.

"We must always make sure that America's soldiers are well-equipped and well-trained to fight this war on terror."

George W. Bush
February 17, 2004

[1] Graduation Address, Texas A&M University, College Station, Texas, August 13, 2004.

TSWG now operates through ten functional subgroups in which participants from diverse backgrounds cooperate to define threats, articulate requirements, and manage the process of technology development to address those threats and requirements. The consensus-based process by which this work has progressed has led to the rapid prototyping of equipment, tools, reference materials, and software that in the words of Secretary of Homeland Security Tom Ridge "have made us better, safer, stronger."

> "The war on terror is a different kind of war, waged capture by capture, cell by cell, and victory by victory. Our security is assured by our perseverance and by our sure belief in the success of liberty. And the United States of America will not relent until this war is won."
>
> President George W. Bush, December 14, 2003

In Fiscal Year 2005, TSWG will continue to ground its program on the four pillars of combating terrorism: antiterrorism, counterterrorism, intelligence support, and consequence management. It will continue to work with over eighty agencies, including the Department of Homeland Security, with which it has established a coherent Science and Technology development agenda. It will continue to meet requirements, one by one, just as the purveyors of terrorism will be taken down cell by cell.

"As enemies continue to adapt and evolve, so must our capabilities."

Donald H. Rumsfeld
August 26, 2004

> "The war on terror is not a figure of speech. It is an inescapable calling of our generation....The only certain way to protect our people is by early, united, and decisive action."
>
> President George W. Bush, March 20, 2004

The pages that follow illustrate TSWG's accomplishments in technology realization during FY 2004. Some products are fully deployed and in use by end users; others remain in some stage of development. There are some projects for which their sensitivity precludes reporting in a public document. Altogether, the following report marks TSWG's continuing vital contribution to the development of suitable technologies and tools to equip our nation's quiver in its determined contest with the global forces of terror.

The Technical Support Working Group

The Technical Support Working Group Subgroups

Appendices

TSWG Organization

In April 1982, National Security Decision Directive 30 assigned responsibility for the development of overall U.S. policy on terrorism to the Interdepartmental Working Group on Terrorism (IG/T), chaired by the Department of State (DOS). The Technical Support Working Group (TSWG) was an original subgroup of the IG/T, which later became the Interagency Working Group on Counterterrorism (IWG/CT). In its February 1986 report, a cabinet-level Task Force on Counterterrorism, led by then Vice-President Bush, cited TSWG as assuring "the development of appropriate counterterrorism technological efforts."

Today, TSWG still performs that counterterrorism technology development function as a stand-alone interagency working group. TSWG's mission is to conduct the national interagency research and development (R&D) program for combating terrorism requirements. It also has commenced efforts to conduct and influence longer-term R&D initiatives and, reflecting the shift to a more offensive strategy, balance its technology and capability development efforts among the four pillars of combating terrorism: antiterrorism, counterterrorism, intelligence support, and consequence management.

Structure

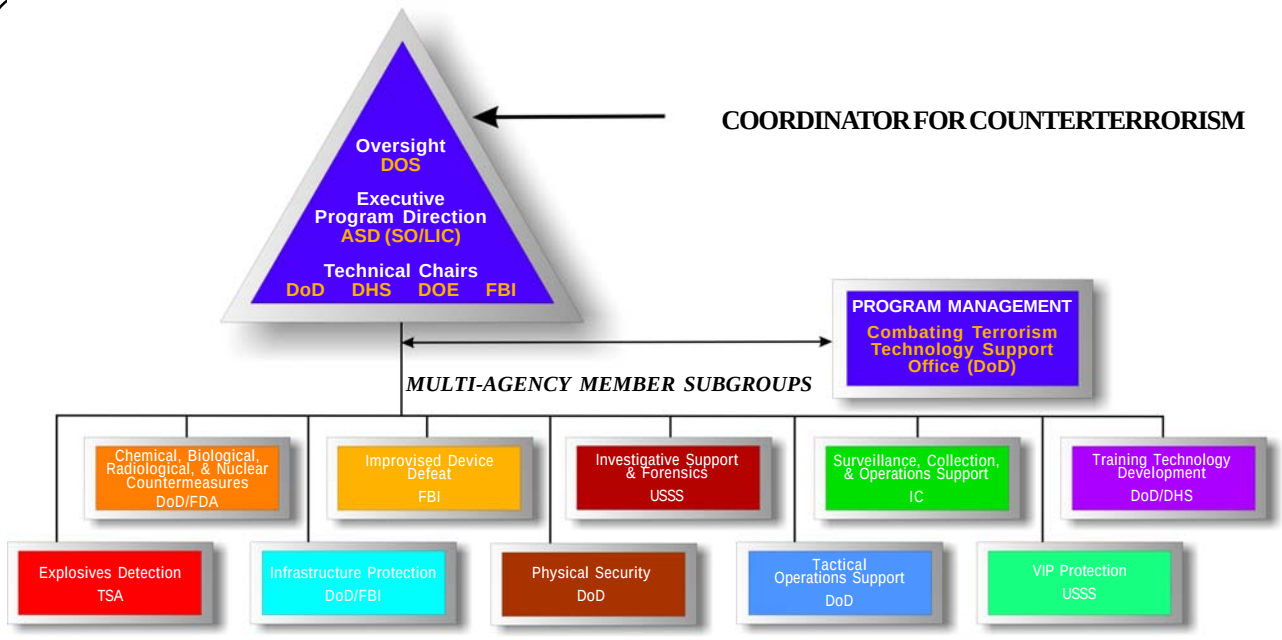
TSWG operates under the policy oversight of the Department of State (DOS) Coordinator for Counterterrorism and under the management and technical oversight of the Department of Defense (DoD) Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict (ASD (SO/LIC)). While TSWG's core funds are derived principally from DoD's Combating Terrorism Technology Support (CTTS) Program and DOS, other departments and agencies contribute additional funds and provide personnel to act as task managers and technical advisors.

As a result of Congressional direction for TSWG to engage in joint counterterrorism R&D efforts with selected NATO and major non-NATO allies, TSWG assumed an international dimension in FY 1993. TSWG conducts cooperative R&D with Canada, Israel, and the United Kingdom through separate bilateral agreements.

TSWG has successfully transitioned capabilities to the Departments of Agriculture, Defense, Justice, State, and Treasury; the Intelligence Community; the Transportation Security Administration; the Public Health Service; and other departments and agencies. Additionally, TSWG has transitioned many systems to State and local law enforcement.

TSWG membership includes representatives from over eighty organizations across the Federal Government. These departments and agencies work together by participating in one or more subgroups. Participation traditionally has been open to Federal departments and agencies, but with the increasing importance of first responders, appropriate representatives from State, local, and international agencies are invited to participate on an as-needed basis. A comprehensive listing of member organizations by subgroup is provided in the appendix.

The ten subgroups are: Chemical, Biological, Radiological, and Nuclear Countermeasures; Explosives Detection; Improvised Device Defeat; Infrastructure Protection; Investigative Support and Forensics; Physical Security; Surveillance, Collection, and Operations Support; Tactical Operations Support; Training Technology Development; and VIP Protection.

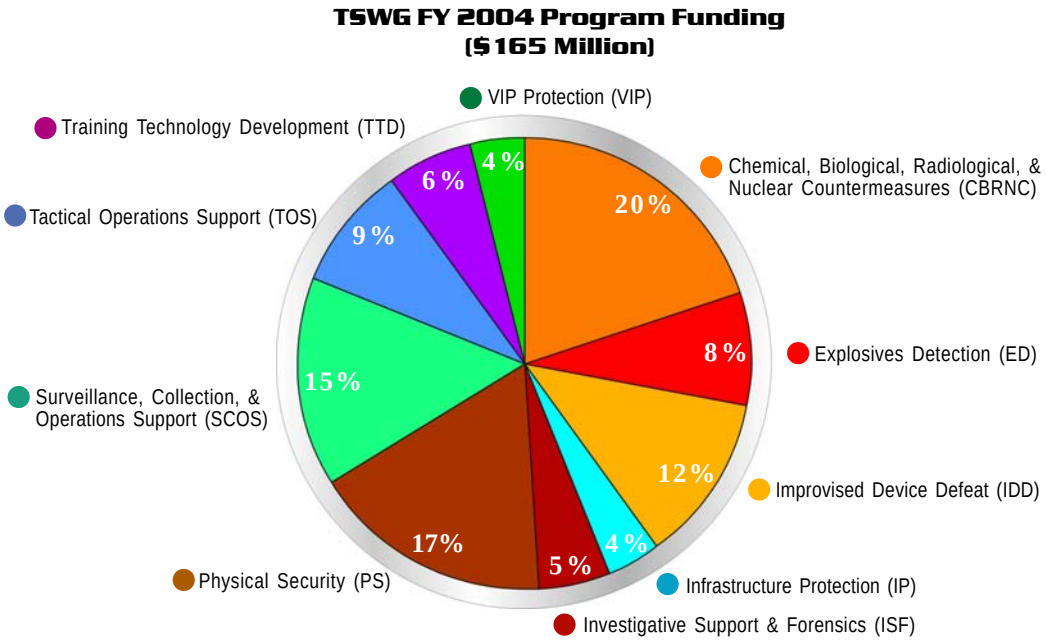


TSWG Organization

Each subgroup is chaired by a senior representative from a Federal agency with special expertise in that functional area. Chairmanship of three subgroups is shared as indicated in the organizational chart above.

TSWG Program Funding

Funding for the TSWG program has increased from almost $8 million in FY 1994 to approximately $165 million in FY 2004. This increase reflects the heightened concern over terrorist activity and the recognized need to accelerate the development of technologies to effectively address the threat. The Department of Defense provides the bulk of funding for TSWG activities; DoD contributed $94 million in FY 2004. The Department of State contributes annually to TSWG core funding, while other departments and agencies share the costs of selected projects.



Mission

Identify and prioritize interagency chemical, biological, radiological, and nuclear combating terrorism requirements and deliver technology solutions for detection, protection, decontamination, mitigation, containment, and disposal.

The Chemical, Biological, Radiological, and Nuclear Countermeasures (CBRNC) Subgroup identifies, validates, and prioritizes multi-agency requirements and competitively seeks technology solutions to counter the terrorist employment of CBRN materials. Through its participation in the InterAgency Board (IAB) for Equipment Standardization and InterOperability and in coordination with DHS, NIJ, and EPA, the CBRNC Subgroup integrates technology requirements from the fire, hazardous materials, law enforcement, and emergency medical services communities. Senior representatives from the Department of Defense and the Food and Drug Administration co-chair the CBRNC Subgroup.

Focus Areas

The CBRNC Subgroup covers the full range of CBRN incident prevention and response to improvised CBRN devices, and the focus areas reflect the prioritized requirements of the CBRN response community. During FY 2004, these focus areas were:

Detection

Improve the sampling, detection, and forensic analysis of chemical, biological, and radiological threat agents in the air, on surfaces, in food, and in water.

Protection

Enhance the operating performance and reduce the costs of personal and building protection CB equipment. Personal Protective Equipment (PPE) includes respiratory protection systems and suits. Building protection includes design tools for engineers in addition to advanced filter materials.

Decontamination

Improve technologies and protocols for personnel, facilities, and equipment decontamination. Systems will be low-cost, environmentally benign, and safe and will be effective for decontaminating chemical and biological warfare agents and persistent toxic industrial chemicals and for mitigation after a release of radioactive materials.

Information Resources

Develop shared information management tools to provide a common "picture of the scene" and facilitate the efficient integration of diverse emergency and consequence management elements from Federal, State, and local agencies.

Membership

Environmental Protection Agency
Fire Department, City of New York
General Services Administration
Mail Policy
Intelligence Community
InterAgency Board
Nuclear Regulatory Commission
U.S. Capitol Police
U.S. Department of Agriculture
APHIS, ARS, FSIS
U.S. Department of Commerce
NIST
U.S. Department of Defense
DIA, DPS, DTRA, JCS, NSA, OATSD/CBD, PFPA, SOCOM, USA (52nd Ord, AMRIID, CMLS, ECBC, FORSCOM, MANSCEN, NGIC, SBCCOM, TEU), USAF (ACC, ESC, FPBL, SG), USMC (CBIRF), USN (NAVCENT, NAWC, NSWC)
U.S. Department of Energy
OS
U.S. Department of Health and Human Services
CDC, FDA, NIOSH
U.S. Department of Homeland Security
BTS (TSA), EPR (FEMA), S&T (HSARPA), USCG, USSS
U.S. Department of Justice
FBI, NIJ, OJP, USMS
U.S. Department of State
DS, OBO, S/CT
U.S. Department of Transportation
Intel
U.S. Postal Service
USPIS
U.S. Senate
SAA
Washington Metropolitan Area Transit Authority

Selected Completed Projects

Personal Heat Stress Calculator

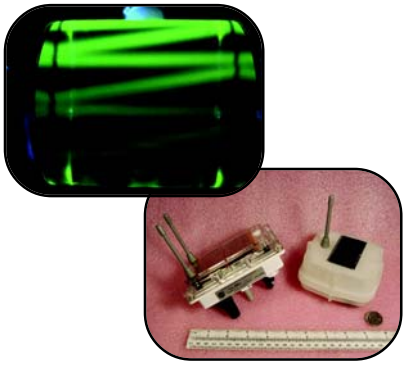
When wearing PPE, users such as first responders to emergency situations are concerned not only with the hazardous agents they may face but also with ancillary issues such as physical stress and overexertion. The Heat Stress Calculator provides a planning tool for first responders to assess and manage heat stress risk while wearing PPE. This personal digital assistant (PDA) allows the user to input workload, PPE configuration, and environmental

Chemical, Biological, Radiological, and Nuclear Countermeasures

conditions into the device to obtain the optimal work/rest cycle for the first responder. The Heat Stress Calculator is commercially available from GEOMET Technologies, Inc. Additional information is available at: www.geomet.com/heatstresspda.com/index.htm

Electrostatic Decontamination System

The proliferation of CB weapons makes it imperative to develop new technologies to provide effective, safe, and efficient decontamination systems to facilitate the timely restoration of operations following a contamination incident. Clean Earth Technologies' portable Electrostatic Decontamination System (EDS) uses a patent-pending decontamination solution, activated by ultraviolet light, to rapidly and effectively neutralize chemical and biological agents with minimal environmental impact and logistical burden. The design is being further improved for increased manufacturability, maintainability, and ruggedness to meet the wide range of operational environments encountered by emergency responders and DoD forces. The EDS is procurement-ready for DoD and other Federal agencies and will be ready for purchase by State and local emergency responders pending EPA registration. Requests for additional information should be sent to cbrncsubgroup@tswg.gov.



Sensor Web

Decontamination of a building after an anthrax release is typically done with chlorine dioxide gas. To maintain effectiveness, the gas concentration, temperature, and humidity throughout the building must be maintained within narrow ranges. Equipped with chlorine dioxide, temperature, and humidity sensors, Sensor Web pods can be efficiently and cost-effectively deployed in a building to monitor the physical conditions and chemical concentrations in real time over the Internet. The communication packages on the pods automatically organize themselves into a wireless network, providing a thinking infrastructure for the sensors they carry. The pods have been deployed for up to 18 months without maintenance using embedded solar cells to recharge the onboard batteries. Additional information and live environmental data from current deployment sites are available at: http://sensorwebs.jpl.nasa.gov.

CB Improvement Building Design Protocol (Web-Based)

Increasing events of domestic and global terrorism have created concerns about potential building vulnerabilities, and methods are needed to safeguard infrastructure and to counter any terrorist deployment of CBRN weapons. To aid in the design or redesign of building collective protection systems, United Technologies Research Center developed a user-friendly software tool to assist building engineers in developing and retrofitting structures against chemical or biological attack. The software performs a vulnerability analysis of a current or planned building, suggests options for decreasing vulnerability, and analyzes the proposed improvement plan. Specific building data, including cost details, can be added by the user. Requests from government agencies for additional information should be sent to cbrncsubgroup@tswg.gov.

Atmospheric Plasma Biological Decontamination System

Neutralizing biological warfare agents on sensitive, high-value items while minimizing material damage is a challenge, with special concern for items of national historical significance. Most currently available technologies damage sensitive items or have considerable logistical hurdles. Atmospheric Glow Technologies (AGT) developed the Atmospheric Plasma Decontamination (APD) system to effectively decontaminate biological spores without producing

significant damage to sensitive materials, such as black and white photographs, cotton-bond printed paper, antique oil paintings, and antique tapestries. The APD system uses AGT's One Atmosphere Uniform Glow Discharge Plasma to create antimicrobial gases that neutralize bioagents without exposing the sensitive items to the liquid chemicals, high humidity, or harsh temperatures associated with other decontamination technologies. AGT is currently developing plans for commercialization of the system. Additional information is available at: www.atmosphericglow.com.

Selected Current Projects

Improved Level A Chemical Protective Ensemble

The increasing threat of international and domestic terrorism has expanded the need for protective clothing within and beyond traditional boundaries. This threat challenges the performance limitations of both civilian and military chemical protective clothing. Current Level A suits require 5 to 10 minutes to don on the scene and only remain effective for approximately one hour. After an hour, chemical, biological, and radiological (CBR) agents can permeate the suit, or the suit may be compromised by exposure to fire or sharp hazards in the environment. Interspiro is developing an improved chemical protective ensemble that provides at least the same level of vapor, aerosol, and splash protection from CBR agents as a National Fire Protection Association (NFPA) 1994 Class 2 ensemble. The ensemble will have improved heat transfer properties and will be compatible with existing commercial and military issued respiratory protection.

Next Generation Fire Fighter Protective Ensemble

With the potential for release of CB agents during terrorist incidents, fire fighters now face additional risks of exposure in which their personal protective clothing does not provide adequate protection. The current generation of PPE is primarily designed to provide protection against the thermal and physical hazards associated with structural fire fighting. The International Association of Fire Fighters and North Carolina State University are designing equipment that will provide protection consistent with the high standards of the NFPA for both structural fire fighting protection and CB protection. These next-generation garments will provide dramatically enhanced protection against chemical and biological agents while improving the flexibility, weight, durability, heat stress reduction, service life, and costs associated with currently available protective gear.

Real-Time Biological Aerosol Detection

Over ten times a second, the bio-aerosol mass spectrometry (BAMS) system developed by Lawrence Livermore National Laboratory samples individual aerosol particles and measures their size and shape. If the particle fluoresces, indicating that it may be of biological origin, a laser fires and hits the aerosol particle, which is traveling at the speed of sound. The ions generated are analyzed by a mass spectrometer to determine the chemical composition. BAMS can distinguish a wide variety of background aerosol particles from those of biological origin. Spores of *Bacillus* can be detected and identified at the species level. *Mycobacterium tuberculosis*, the cause of TB, can also be identified, providing a dual-use application for the technique in the public health domain.

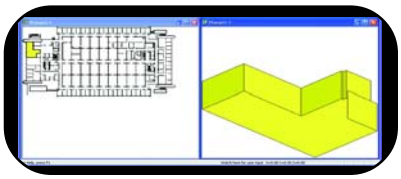
Distributed Chemical Sensor

Monitoring a facility or building with a collection of point chemical sensors is expensive, can leave gaps in coverage, and delays the alarm since the toxic

cloud must move to the sensor. The Distributed Chemical Agent Sensing and Transmission (DiCAST) system under development by Intelligent Optical Systems replaces these point sensors with a continuous line of protection. DiCAST integrates stable and sensitive reagents for the rapid detection of selected toxic industrial chemicals and CWAs into the plastic cladding of specially designed and drawn optical fibers. By deploying the sensing fiber cables in buildings and on the perimeter of facilities, base and facilities security managers can monitor, detect, and warn of a chemical attack. The sensing fibers respond to the presence of the toxic chemical in seconds, and the alarm moves along the fiber at the speed of light. The first field evaluation will be conducted in Spring 2005.

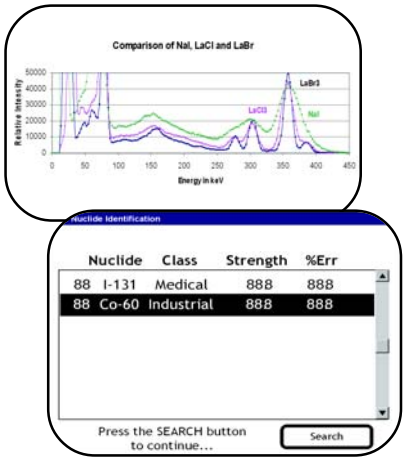
Expedient Mitigation of a Radiological Release

To mitigate the effects of terrorist use of a radiological dispersion device, rapid containment of radioactive material is essential. First responders need materials, equipment, and procedures to remove radioactive surface contaminants quickly and efficiently. Isotron is developing a novel coating technology and process for immediate countermeasures that will support crisis response in the aftermath of a radiological release. The technology will provide a critical capability to first responders to prevent the unwanted spread of radionuclides and to facilitate subsequent restoration and decontamination efforts.



Statistical Design Tool for Sampling Contaminated Buildings

Ensuring the success of building decontamination following a chemical or biological event requires a statistically valid surface sampling plan for determining the extent of contamination. Pacific Northwest National Laboratory (PNNL) is developing a software tool to guide the efforts of response personnel in sample collection and decontamination efficiently and effectively. PNNL is enhancing the capabilities of an existing software package, the Visual Sample Plan (VSP), which enables decision makers to quickly create a sampling plan that allows them to define with high confidence the magnitude and extent of contamination, guide decontamination efforts, and verify the effectiveness of decontamination. The enhanced VSP will advise consequence management and emergency responders on how best to assess the contamination and to evaluate decontamination efforts.



Real-Time Radioisotope Identification and Reporting

Border security and public safety personnel at all levels of government need to quickly, reliably, and affordably distinguish radioactive threat materials from the many naturally occurring, industrial, and medical radioisotopes moving in commerce. SAIC's Advanced Radioisotope Identification System (ARIS) integrates a new room-temperature scintillation crystal with twice the resolution of the material used in existing isotope identifiers. Better resolution will result in faster and more confident identification for border security, bomb squad, and hazardous materials response units. Support for backup analysis is built into the system. The integrated global positioning system (GPS) and wireless data transfer capabilities facilitate the transfer of annotated high resolution gamma spectra from remote incident locations to analysis and command centers over existing telecommunications paths. ARIS is being built and tested to meet ANSI N42.34, which is a standard for performance criteria for handheld instruments for the detection and identification of radionuclides.

Contact Information

cbrncsubgroup@tswg.gov

Mission

Identify, prioritize, and execute research and development projects that satisfy interagency requirements for existing and emerging technologies in the area of explosives detection and diagnostics. Emphasis is placed on a long-term, sustained approach leading to new and enhanced technologies for detection and identification of improvised explosive devices and large vehicle bombs.

These projects are intended to enhance the operational capability of both military and civilian applications. A representative from the Transportation Security Administration chairs the ED Subgroup.

Membership

U.S. Capitol Police

U.S. Department of Defense
DIA, NSA, USA (TEU), USAF (ACC, AFRL, ESC), USN (NAVEOTECHDIV, NCIS, NRL)

U.S. Department of Energy
OS

U.S. Department of Homeland Security
BTS (CBP, FAMS, FPS, TSA), S&T (HSARPA), USCG, USSS

U.S. Department of Justice
ATF, NIJ

U.S. Department of State
DS

U.S. Postal Service
USPIS

Focus Areas

The ED Subgroup focus areas reflect the prioritized requirements of a broad range of interagency customers, including those responsible for physical security and forensic analysis. During FY 2004, these focus areas were:

Large Vehicle Bomb Detection

Develop technologies necessary to provide a stand-off detection capability of explosives in large volumes at greater distances. This includes investigating unique physical and chemical phenomena that identify the presence of explosives, the physical limits for sensor technology to respond to these phenomena, and enhancements to detection technology. To provide near-term solutions, ED is developing remote detection techniques, where a system can be downfield from the operator but near the objects of interest. Long-term technologies leading to a true stand-off capability are being explored.

Suicide Bomber Detection

Improve systems that detect the presence of improvised explosive devices concealed by persons engaged in suicide attacks against government installations and public facilities, both domestic and international. Programs in this area are highly sensitive; specific capabilities generally cannot be discussed in an open document.

Short-Range Detection

Develop new explosive detection capabilities and improvements to existing systems for detection and diagnosis of concealed terrorist devices. Emphasis is placed on technology areas that lead to equipment development for entry-point screening. Key areas include improvements in detection rate, throughput, and accuracy in identification of explosives, as well as safety for both operators and the general public.

Canines

Develop training tools, protocols, and technologies that support and enhance canine detection of explosives. The goal is to improve canine team effectiveness and consistency through better understanding of both canine detection ability and canine/human interaction.

Completed Projects

Increasing Marking Agent Concentration in Flexible Sheet Explosives

Marking agents are chemicals added to plastic explosives to make them more detectable. This project compared the manufacturing process, explosive

performance characteristics, and operational use of flexible sheet explosives containing either no marking agent, the current concentration, or an increased marking agent concentration. Testing in both a military and civilian application found no significant differences in performance between the three versions of flexible sheet explosives. Handling and manufacturability of the explosives were acceptable in all cases. The report recommends further study of workplace exposures to the marking agent during manufacturing. Results were presented to the International Civil Aviation Organization in September 2004. Requests for additional information should be sent to edsubgroup@tswg.gov.

Housing and Husbandry of Canines

The importance of canine detection, the investment in training, and the close relationships developed between dogs and handlers call for careful attention to animal welfare before, during, and after detection training. This study identified appropriate definitions of animal welfare for detection dogs, factors causing stress in kenneled dogs, means of measuring canine stress, and the effects of stress on canine performance. It also includes simple improvement measures, such as providing raised sleeping platforms for kenneled dogs. A previous study provided metrics that may be used to select dogs for bomb detection training. Results of both studies will be included in mandatory training manuals for service dogs in the United Kingdom. These projects have provided a practical scientific basis for this keystone of canine detection and are useful for both existing and new programs. Requests from government agencies for these reports should be sent to edsubgroup@tswg.gov.

Current Projects

Canine Handler Selection

Researchers in both the United States and the United Kingdom, with the involvement of agencies that use canines for detection, are developing selection methods and training materials for canine handlers. A handler selection program based on this research will enhance the efficiency of training programs by decreasing attrition. Better methods of selecting handler trainees, combined with a strong training program, will raise the overall skills and performance of canine handlers. Three surveys of both experienced and trainee handlers to identify their personality traits and attitudes towards dogs are in progress.

Neutron Generator Technology for Explosives Detection in Cargo and Vehicles

Lawrence Berkeley National Laboratory is building an advanced neutron generator that will enable development of systems for automated, non-intrusive detection of explosives in cargo containers, wrapped pallets, railcars, and vehicles. Long-lasting neutron sources are an essential enabling technology for large vehicle bomb detection. This generator is expected to have a lifetime exceeding 1000 operating hours at full output. Neutron activation analysis systems based on this generator will be suitable for fixed installations at both commercial and military sites while being compact enough to deploy.

Quadrupole Resonance Personnel Screening Portal

Quantum Magnetics has developed a prototype Quadrupole Resonance (QR) portal for the detection of explosive devices concealed on persons. QR technology provides a capability to directly detect bulk explosives that have been problematic

for trace methods. One prototype integrated with an advanced metal detector has been built, and two more are currently being assembled. The first prototype is being readied for use in an operational assessment by the Transportation Security Administration. This non-trace explosive detection system for personnel screening may be integrated with a trace portal for additional capability, or used in locations where trace detection is not viable because of high background levels of dirt or chemicals.

Trace Explosive Detection Using Handheld Chemical Analyzer

Defence Science and Technology Laboratories is developing a handheld mass spectrometer for trace detection of explosives. The device will use a solid-state sensor and have high specificity, providing identification of particular explosive compounds. The design goal is identification of 1 Atomic Mass Unit (AMU) differences for compounds up to 400 AMU. Detector chips for the prototype have been delivered and are being tested.

Contact Information

edsubgroup@tswg.gov

Mission

Identify, prioritize, and execute research and development projects that satisfy interagency requirements to more safely and effectively render terrorist devices safe. Particular emphasis is placed on technologies to access, diagnose, and defeat terrorist improvised explosive devices (IEDs); improvised CBRN devices; and vehicle-borne improvised explosive devices (VBIEDs).

The Improvised Device Defeat (IDD) Subgroup delivers advanced technologies, tools, and information to increase the operational capabilities of the U.S. military explosive ordnance disposal (EOD) community and Federal, State, and local bomb squads to defeat and mitigate terrorist devices. In collaboration with military, Federal, State, and local agencies, the IDD Subgroup identifies and prioritizes multi-agency user requirements through an ongoing process. A representative from the Federal Bureau of Investigation's Bomb Data Center chairs the IDD Subgroup.

Membership

Fairfax County (VA) Police Department
Intelligence Community
National Bomb Squad Commanders Advisory Board
U.S. Capitol Police
U.S. Department of Defense
USA, USAF, USMC, USN
U.S. Department of Homeland Security
BTS (ODP, TSA), IAIP, S&T (HSARPA), USSS
U.S. Department of Justice
ATF, FBI, NIJ, USMS

Focus Areas

The IDD Subgroup focus areas reflect the joint priorities of military and civilian responders. During FY 2004, these focus areas were:

Access & Diagnostics

Develop advanced technologies for diagnostic analysis of IEDs in the areas of improved tools and equipment. Projects in this area develop technologies to access and accurately locate and/or identify components and composition within an improvised terrorist device to facilitate timely response and device neutralization.

Defeat

Develop advanced technologies to defeat IEDs, VBIEDs, and improvised CBRN dispersal devices. Emphasis is placed on developing low-cost solutions that are readily available to the bomb squad community. This focus area includes projects that are designed to increase stand-off capabilities, reduce collateral damage, and provide precision disruption and disablement capabilities and techniques.

Tactical Tools

Develop improved tools and equipment to increase the safety and effectiveness of EOD and bomb squad technicians during a response. Projects in this field provide enhanced situational awareness, improved tactical tools, and tools to counter emergent explosive threats.

Information Resources

Develop information resources and delivery systems to enhance response capabilities. This area provides equipment performance results, database resources, operational response technology information, and automated information systems to improve tactical and operational response capabilities.

Remote Controlled Vehicles and Tools

Develop technologies that will improve the performance and reliability of robotic systems for the bomb squad technician. These technologies include advanced robotic platforms with improved manipulation capabilities, control systems, navigation technologies, payloads, and communications. TSWG's Common System Architecture is the foundation of these systems and will for the first

time enable all robotic components, regardless of the developer, to be "plug-and-play." With the increasing diversity and complexity of terrorist threats, it is vital that the bomb technician conduct as much of the mission as possible by remote means.

Emergent Threats

Characterize improvised explosive mixtures used by terrorist organizations and develop effective response procedures, tools, and equipment to counter the threat.

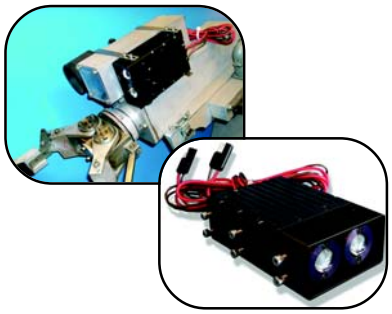
Selected Completed Projects

Suicide Bomber Response Standard Operating Procedures and VBIED CD-ROM Reference Database and Guideline Standard Operating Procedures

The Suicide Bomber Response Standard Operating Procedures (SOPs) provide consensus-based response protocols for Federal, State, and local bomb squads and first responders. The protocols include the minimum essential information, knowledge, tools, and procedures needed to prepare for, respond to, and mitigate the consequences of suicide bombers and bombs in the United States. The VBIED CD-ROM Reference Database and Guideline SOPs are recommended tactics, techniques, and procedures to counter the threat represented by VBIEDs. The SOPs are a compilation in CD-ROM format of the knowledge, experience, and expertise of U.S. and international partners for combating these threats. The SOPs promulgate relevant technology and intelligence to assist bomb squads and first responders with training programs and policy development. The CD-ROMs are available for distribution to accredited bomb squads and first responders throughout the United States. Requests from government agencies for additional information should be sent to iddsubgroup@tswg.gov.

Stand-Off Connectivity Control Unit

The bomb squad and EOD communities required a product that allows for the easy adaptation of existing digital equipment, such as the RTR-4 X-ray imaging system and the ADM-300 radiological monitor, to analog robotic platforms. The Stand-Off Connectivity Control Unit (SCCU) was developed to provide backward compatibility of existing sensor technology with legacy analog robotic systems. It will increase the remote capabilities without costly robotic modifications. Additional information on the SCCU can be obtained from Nomadics by sending requests to contacts@nomadics.com.



Robotic White Light/Infrared Switching System

Currently, robotic platforms solely use incandescent white light for bomb squad operations. While these lights provide vehicle-mounted cameras enough light to operate, they are not ideal for use in tactical situations. This completed effort provides existing and new robotic platforms with enhanced lighting capabilities that can be switched from a white spotlight to a low-level infrared light as the response dictates. Additional information on this product can be obtained by completing a Web inquiry form at the QinetiQ Web site: www.qinetiq.com.

Radio Frequency Remote Firing Device Upgrade

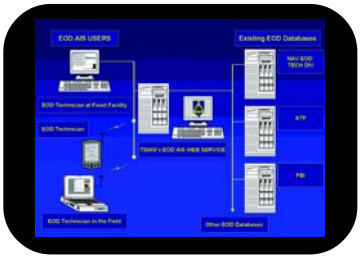
The commercial Radio Frequency Remote Firing Device (RFD) previously developed by TSWG is a low-cost, lightweight, battery-operated firing system used by civilian law enforcement personnel for firing electric detonators, electrically primed cartridges, blasting caps, and an explosive shock tube in the

performance of render-safe procedures. The U.S. Air Force requested an upgrade to the RFD to meet the operational requirements of deploying EOD teams. This effort incorporated recommended changes identified during an Operational Utility Evaluation of the RFD system. The upgraded system provides the EOD community with an extremely rugged, low-cost firing system. Additional information on this product can be obtained from Engineering Technology, Inc. at: www.engrtech.com.

Selected Current Projects

EOD Automated Information System

The Automated Information System will enable EOD operators and bomb technicians to search, retrieve, and exchange information across numerous networks and systems from a fixed facility or from a laptop in the field. This Web-based system will allow responders to rapidly access information, render-safe procedures, and disposal options for improvised explosive devices. The next development effort will focus on preparing this system for deployment and use by State and local bomb squads and first responder communities.



First Responder Automated Data Tool Real-Time Information Sharing System

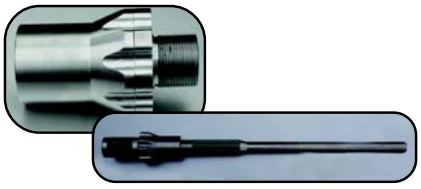
Bomb disposal technicians and other first responders need to actively share intelligence and situational awareness information in real time. The current First Responder Automated Data Tool (FRAT) system provides users with a common application to organize, share, and store reference materials, information, graphics, and applications. The sharing of information is limited to local users within the department. This effort will integrate standards recently adopted by the NIJ into the existing FRAT system, providing bomb disposal technicians with the ability to publish information and to query critical information that has been published by other bomb disposal personnel and government agencies. This task will be accomplished by the integration of the FRAT Real-Time Information Sharing system into the existing Law Enforcement Online (LEO) system and the Bureau of Alcohol, Tobacco, Firearms, and Explosives Bomb and Arson Tracking System (BATS) to allow the nationwide sharing of information throughout the bomb squad and first responder communities.

Next-Generation Explosive Ordnance Disposal Remote Controlled Vehicles and Tools

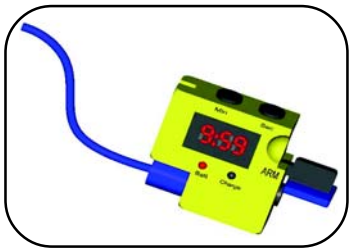
Using TSWG's Common System Architecture for modular "plug-and-play" capability, iRobot has successfully developed and demonstrated advanced remote controlled vehicle technology subsystems for explosive ordnance disposal. These subsystems include semiautonomous mobility, advanced manipulator cooperative behaviors, and automatic pay-in/-out tensionless fiber-optic systems having over 1 km range. Also included are wireless communications with the capability of two-way audio and video transmission and an automatic recovery protocol in the event of loss of signal. Efforts will continue into subsystem integration testing onto an advanced mobility platform.

Recoilless Disruptor Breech Characterization

Bomb disposal technicians use robotic platforms to remotely position and fire explosively driven disrupters against IEDs to access or defeat these devices. The high recoil forces of these disrupters have caused damage to the manipulator system of the robotic platform. A Recoil Reduction Adapter has been developed by the manufacturer of the Percussion Actuated Non-electric (PAN) disruptor



and was stated to greatly reduce the recoil force. This project addresses characterization testing of the developed adapter. This testing will confirm the degree of reduction in recoil forces as well as loss of muzzle energy and will verify that cartridge characteristics are unaffected.



Tactical Timed Firing Device

To initiate energetic charges and tools under controlled situations, military EOD and bomb disposal communities need a small, reliable, easy-to-use, multi-use, and self-contained timed firing device. The Tactical Timed Firing Device (TTFD) will fire multi-sized shock tubes, electrical blasting caps, or electrically primed cartridges during EOD or bomb squad response situations. The TTFD will be ready for use in under a minute, use standard battery power, and operate in extreme climactic conditions. Additionally, the TTFD will provide an alternative to radio frequency remote firing devices in situations where the use of radio frequency transmissions is prohibited.

Contact Information

iddsubgroup@tswg.gov

Mission

Identify, prioritize, and execute research and development projects that satisfy interagency requirements for the protection and assurance of critical Government, public, and private infrastructure systems required to maintain the national and economic security of the United States.

The Infrastructure Protection (IP) Subgroup works to ensure the uninterrupted service of infrastructure systems that are vital to maintaining the national and economic security of the United States. These critical systems include control systems for electric power, natural gas, petroleum products, and water; telephone, radio, and television; ground, rail, and air transportation facilities; and cyber communications networks. IP research and development reflects the multivariate threat to the complex and interdependent systems, subsystems, and components of the nation's infrastructure. Solutions include conventional security measures plus those offered by emerging technologies. Representatives from the Department of Defense and the Federal Bureau of Investigation co-chair the IP Subgroup.

Membership

Environmental Protection Agency
Nuclear Regulatory Commission
U.S. Department of Agriculture
FS
U.S. Department of Commerce
NIST
U.S. Department of Defense
DTRA, JPO-STC, USA (CE), USAF (OSI), USMC (CIP), USN (NCIS, NSWC)
U.S. Department of Energy
OEA, OS
U.S. Department of Homeland Security
BTS (FPS, ODP, TSA), EPR (FEMA), S&T (HSARPA, NIPC), USSS
U.S. Department of Justice
FBI
U.S. Department of Transportation
FAA, Volpe

Focus Areas

The IP Subgroup focus areas reflect the prioritized requirements generated with respect to critical aspects of the nation's infrastructure. During FY 2004, these focus areas were:

Cyber Security

Provide detection, prevention, response, and alert capabilities to counter cyber attacks and harden computer systems. Society increasingly relies upon new information technologies and the Internet to conduct business, manage industrial activities, engage in personal communications, and perform scientific research. The complexity and sophistication of information technologies and their widespread integration increases the likelihood of unforeseen vulnerabilities. Unprecedented opportunities are created for criminals, terrorists, and hostile foreign nation-states to steal money or proprietary data, invade private records, conduct industrial espionage, or cause failure of vital infrastructure elements. The prevention and mitigation of threats to computer networks is vital in almost all its facets.

Information Analysis

Develop tools and methodologies to support analysts who are overwhelmed by the volume, variety, and velocity of information that must be processed. Information analysis technologies enhance the storage, protection, analysis, discovery, and presentation of disparate sources of data in meaningful forms.

Physical Protection

Standardize methodologies and decision aids for vulnerability analysis and enhanced protection of critical elements to secure the nation's infrastructure. These elements include power generation and transmission, water supplies, and health services. By understanding the dynamics of complex critical infrastructures, secure operating methodologies and strategies can be developed to prevent and mitigate widespread failures caused by cascading and interactive network effects. This research will evaluate dynamic behavior models, develop common standards and practices in and between critical infrastructures, and investigate system vulnerabilities to various threats.

Selected Completed Projects

Network Isolation Tool

The Network Isolation Tool provides an early indication of when to sever connections between local area networks (e.g., internal mission critical, administrative) and wide area networks (e.g., external networks, the Internet). The system is capable of remote operation and contains internal intrusion detection based on behavioral modeling. Additional information can be found at: www.psynapsetech.com/checkmate_ips.html.

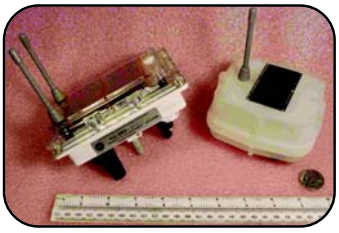
American Gas Association Standard for Supervisory Control and Data Acquisition

The American Gas Association (AGA) 12-1 is a standard for the encryption of Supervisory Control and Data Acquisition (SCADA) communications that can be adopted by utility companies to secure interactions between master systems and remote terminal units in the field. Systems built to the AGA 12-1 standard are National Institute of Standards and Technology compliant and provide the latest in secure communications for SCADA systems and deny unauthorized data transmissions or intrusions. The latest version of AGA 12-1 and the Java code that implements the standard can be found at: www.gtiservices.org/security/aga12_wkgdoc_homepg.shtml.

Supervisory Control and Data Acquisition Cryptographic Module

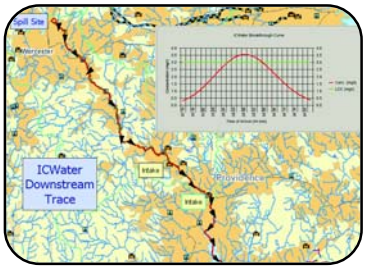
Developed by the Gas Technology Institute, the SCADA cryptographic module encrypts communications between components of a SCADA network to protect against hackers or other misuse. The SCADA cryptographic module complies with AGA 12-1 for natural gas systems and can also be used for water and electric power SCADA systems. Additional information can be found at: www.gtiservices.org/security/index.shtml.

Selected Current Projects



Sensor Web for Infrastructure Protection

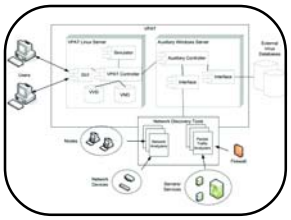
The Sensor Web for Infrastructure Protection (SWIP) is a wireless sensor web equipped with tilt meters that will be mounted on towers, detect when the towers are falling over, and report back to a central monitoring location. This system is an extension of the Sensor Web project initiated by the CBRNC Subgroup. The SWIP can be equipped with various types of sensors depending on the application to protect other critical infrastructure.



Incident Commanders Water Modeling Tool

The Incident Commanders Water Modeling Tool (ICWater) will extend the capability of the previously developed RiverSpill modeling tool to allow an incident commander to analyze and react quickly to chemical and/or biological contaminants introduced into surface water sources. The number of river segments covered will expand from 68,000 to over 3 million river segments nationwide. In addition, ICWater will be "plug-and- play" with existing incident commander and emergency response tools such as the Chemical Biological Response Aide (CoBRA), Consequence Assessment Tool Set (CATS), Natural Hazard Loss Estimation Methodology (HAZUS), and the EPA Emergency Response Analyzer.

Virus Propagation Analysis Tool



The Virus Propagation Analysis Tool (VPAT) is being developed to assist system administrators in planning and protecting their communication networks from the harmful effects of malicious code by providing a better understanding of how viruses propagate across the Internet. The tool will analyze the severity of infection, identify weak points in a network's defense, and suggest strategies for recovery and mitigation.

Supervisory Control and Data Acquisition Protocol Vulnerability

The SCADA protocol vulnerability system will provide a rapid means to test critical SCADA network components for both known and unknown security flaws prior to deployment. SCADA is used extensively by the energy industry (e.g., gas, oil, electric, water), and the initial capability of this system will be to test the Modbus protocol, which is currently the most prevalent in the industry.

Contact Information

ipsubgroup@tswg.gov

Mission

Identify, prioritize, and execute research and development projects that satisfy interagency requirements for criminal investigation, law enforcement, and forensic technology applications in terrorism-related cases.

The Investigative Support and Forensics (ISF) Subgroup supports research and development projects that provide new capabilities to law enforcement personnel, forensic scientists, and intelligence operatives responsible for investigating and interdicting terrorist incidents. Projects conducted through this group have had a major impact on forensic investigations and intelligence operations throughout the law enforcement community. A representative from the U.S. Secret Service chairs the ISF Subgroup.

Membership

Environmental Protection Agency
CID, NEIC
Federal Reserve Board
Intelligence Community
National Transportation Safety Board
U.S. Department of Commerce
NIST (OLES)
U.S. Department of Defense
AFIP, DARPA, DCFL, DoDPI, DTRA, NSA, USA (CID), USAF (OSI), USMC (CBIRF), USN (NCIS)
U.S. Department of Energy
OS
U.S. Department of Homeland Security
BTS (CBP, FDL, FPS, TSA), EPR (FEMA), S&T (HSARPA), USSS
U.S. Department of Justice
ATF, DEA, FBI, NIJ (NCFS, NFSTC), USMS
U.S. Department of Transportation
FAA
U.S. Postal Service
USPIS

Focus Areas

The ISF Subgroup focus areas reflect the prioritized requirements of the military and civilian law enforcement communities. During FY 2004, these focus areas were:

Crime Scene Response

Improve the quality of evidence recognition, documentation, collection, and preservation, as well as the protection of examiners from hazardous materials exposure. Additionally, training of first responders and forensic examiners at terrorist incident scenes is addressed in this area. This focus area also includes scientific and technical efforts not otherwise assigned to other ISF focus areas.

Electronic Evidence

Develop computer forensic hardware, software, decryption tools, and digital methods to investigate terrorism. New projects in this field are also developing advanced methods to extract and enhance audio recordings and video images from surveillance sources. This area includes identifying computer systems and media used by terrorists and extracting the maximum amount of evidence from them.

Explosive and Hazardous Materials Examination

Improve methods for assessing the size, construction, and composition of explosive devices or other energetic hazardous materials. This area also emphasizes the identification and analysis of explosive residue and other trace evidence present at blast scenes, especially those requiring rapid protection and processing, to preserve the evidentiary value.

Forensic Biochemistry

Develop analytical methods used on biological evidence found at terrorist scenes to make identifications and extract information such as origin or age. The use of DNA to identify or profile persons receives special interest because of its highly discriminative and sensitive properties. This focus area also looks at locating the geographic origin of organic material based on their stable isotope ratios.

Friction Ridge Analysis

Improve latent print techniques used in terrorism cases. Emphasis is given to processes involving the automation of multiple techniques that are tedious, expensive, non-portable, or use hazardous chemicals. This encompasses efforts to create better visualization and development of latent prints using lasers or more versatile and affordable reagents. Other areas of interest are the better

comprehension of latent prints and their molecular content, as well as the scientific validation of fingerprint examinations.

Questioned Document Examination

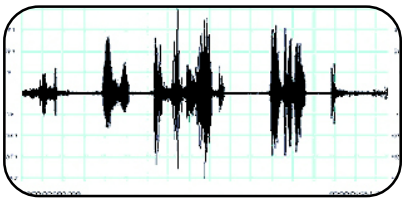
Develop advanced document and handwriting analysis techniques, devise standardized identification criteria, and establish a legal scientific basis for these examinations. Questioned document examinations include forgeries, tracings, disguised handwritings, and writing in different languages and character sets. Development of software for identifying counterfeit documents and matching documents by handwriting analysis and pattern recognition algorithms also fall under this focus area.

Surveillance Technology

Produce new and advanced surveillance devices for law enforcement use. These technologies are categorized by the nature of the technology (e.g., infrared, X ray, visual, audio/speech), the type of data derived (e.g., visual, aural, digital), or the awareness of the target being surveilled. This focus area includes projects that improve polygraphy and develop new methods or equipment for the detection of deception. Development under this focus area is closely coordinated with the SCOS Subgroup.

Selected Completed Projects

Improved Audio Tape Enhancement

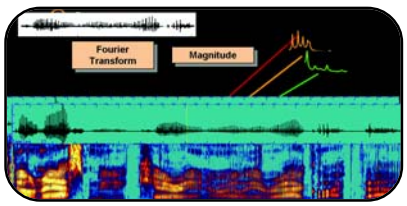


Investigators commonly receive poor quality audiotapes requiring speaker separation or elimination of random noise. This software tool uses the most advanced signal processing algorithms available to overcome these difficulties. These methods can also be used to enhance recordings from other types of storage media after converting them to commonly used .wav files. These processes are often used in conjunction with the Reliable Audio Voice Identification software, also developed by the Massachusetts Institute of Technology's Lincoln Laboratory. Requests for additional information should be sent to isfsubgroup@tswg.gov.

Improved Video Tape Enhancement

Videotapes submitted for forensic examination are often the result of inferior equipment or inadequate recording conditions. Poor video taping conditions include low light level, out-of-focus lens, and motion blur. New videotape enhancement algorithms and processes that produce final videotapes of evidentiary quality compensate for these defects. This software is commercially available from Signalscape, Inc. at: www.signalscape.com/forensics.htm.

Reliable Audio Voice Identification



Typical voice comparison systems require consistent or well-controlled collection parameters that are unrealistic in the forensic environment. Real-world recordings may be over varied channels, in the presence of competing noise or speakers, or even recorded while the speaker is under duress. The Massachusetts Institute of Technology's Lincoln Laboratory developed an advanced voice identification system and reference for use in forensic casework. The system compares a new or unknown voice sample to a collection of known voice samples. Different voices saved on various storage media and recorded under diverse conditions can be compared, and unwanted noise can be eliminated. Phone-based speaker recognition technology is also included in this system. Requests for additional information should be sent to isfsubgroup@tswg.gov.

Questioned Identification Document and Link Database

Terrorists and their supporters often use false or forged identity documents to cross international borders. The Questioned Identification Document and Link Database is a centralized reference merging existing Federal and ICPO-Interpol databases of genuine and counterfeit identification documents (passports, driver's licenses, credit cards). The system permits real-time comparison of suspect documents with images of genuine and other known counterfeit documents. It also provides comprehensive information on specific features to determine the authenticity of suspect documents, as well as link analysis data on similar cases. Access to the system is available through the U.S. Secret Service, who provided most of the existing databases. Requests for additional information should be sent to isfsubgroup@tswg.gov.

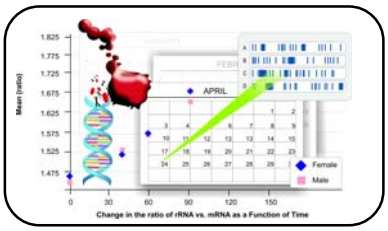
Link Analysis of Computers and Media with Reachback Signals

Procedures and equipment are needed to associate storage media with an individual disk drive and an individual computer. This capability was accomplished using modulation signals within the computer. Additionally, the capability was developed to forensically link a target computer (e.g., a laptop, desktop, or network server) to an attempted or actual penetration of a U.S. Government computer network. These techniques established the capability to classify and identify the individual characteristics of a computer or storage media to form a link between the questioned and known equipment. Requests for additional information should be sent to isfsubgroup@tswg.gov.

Selected Current Projects

Age Determination of Biological Evidence

Researchers at West Virginia University are developing a forensic method to determine the specimen age of recovered biological evidence. They will compare rates of RNA breakdown in a biological sample to estimate the time since its deposition. This project is also investigating how the decay rates are affected by environmental variables such as temperature, humidity, recovery surface, and inter- and intra-population variability.



Remote Polygraphy Using Laser Doppler Vibrometry

Formal polygraph examinations are impractical in many combating terrorism scenarios. Techniques are needed that will allow law enforcement officials to quickly and surreptitiously detect deception in many different environments, thus decreasing the ability of a suspect to employ countermeasures. Remote Polygraphy Using Laser Doppler Vibrometry (LDV) is an advanced physiological recording system for use in the detection of deception and the assessment of threat and credibility. LDV is a non-contact method of deception analysis that can be used at stand-off distances of several meters. This technique will allow law enforcement officials to quickly and surreptitiously detect deception in many different environments, particularly at ports of entry.

Wireless Phone and PDA Toolkit

A field-deployable forensic examination tool is being developed to extract data from wireless telephones and personal digital assistants (PDAs). This toolkit will allow an investigator to access, read, and copy stored data from wireless telephones and PDAs while protecting the integrity of the evidence. The application will identify the stored information on these devices and then download it to another computer without leaving any trace on the targeted device.

Long-Range Non-Line-of-Sight Wireless Video Transmission System
Covert video surveillance is difficult in dense urban environments. The Long-Range Non-Line-of-Sight Wireless Video Transmission System uses novel digital transmission techniques to overcome the shortcomings of current analog systems. This digital transmission system performs well in dense urban environments because it provides a video signal that overcomes high interference and ghost imaging. The system is expected to have a range of five miles and will be interoperable with commonly used police surveillance cameras and recording equipment.

Contact Information

isfsubgroup@tswg.gov

Mission

To identify and execute research and development projects that satisfy interagency requirements for physical security support to protect personnel, equipment, and facilities against terrorist attack.

The Physical Security (PS) Subgroup identifies the physical security requirements of government agencies both within the United States and abroad and develops technologies to protect personnel and property from terrorist attacks. The Subgroup develops these technologies by creating prototype hardware, software, and systems for technical and operational evaluation by user agencies. A Department of Defense representative from the U.S. Naval Forces Europe chairs the PS Subgroup.

Focus Areas

The PS Subgroup focus areas reflect the prioritized requirements of the physical protection community. During FY 2004, these focus areas were:

Blast Mitigation

Develop blast mitigation technologies necessary to address blast debris hazards and prevent structural collapse, the primary causes of injury and death. This focus area seeks design and construction solutions for new buildings, as well as retrofit techniques for existing structures.

Entry Point Screening

Develop multiple technologies and techniques to detect explosives; weapons; chemical, nuclear, or radiological material; and other contraband on personnel or in vehicles, vessels, cargo, or mail entering protected facilities. Solutions are intended to increase detection rates, throughput, and safety while reducing the number of security forces required to perform the screening process.

Intrusion Detection, Assessment, and Delay

Develop improved intrusion detection systems, video alarm-assessment systems, specialized intrusion-delay barriers, and subsequent armed response capabilities for protecting outer perimeters, building perimeters, and key assets from terrorist attacks. This focus area emphasizes prototype security systems with increased or improved capabilities and lower operation and maintenance costs.

Membership

Federal Reserve Board
Intelligence Community
National Aeronautics and Space Administration
Nuclear Regulatory Commission
Port Authority of New York/ New Jersey
Supreme Court of the United States
U.S. Department of Defense
CENTCOM, DTRA, EUCOM, JCS, JFCOM, NSA, OUSD/AT&L, USA, USAF, USMC, USN
U.S. Department of Energy
NNSA, OS
U.S. Department of Homeland Security
BTS (CBP, FLETC, TSA-M&LS), S&T (HSARPA), USCG, USSS
U.S. Department of Justice
ATF, FBOP, NIJ
U.S. Department of State
DS
U.S. Department of Transportation
OIS
U.S. Postal Service
USPIS

Selected Completed Projects

Polymer Retrofit Coating System

The U.S. Marine Corps desired greater protection for High-Mobility Multipurpose Wheeled Vehicles (HMMWVs) in the U.S. Central Command (CENTCOM) equipped with standard armored doors made from 0.202" high hard steel (HHS). Although 3/8" rolled homogeneous armor (RHA) is more effective, it was not available at the time. TSWG sponsored the development of a two-part, spray-on retrofit coating to increase the level of protection offered by the 0.202" HHS to equal or exceed that of the 3/8" RHA. The resulting protection offered by the retrofitted 0.202" HHS equals, and in some ways exceeds, the performance of the 3/8" RHA and provides a weight savings of approximately 1.6 lbs per square foot. At time of printing, approximately 96 doors had been retrofitted and are in use in CENTCOM. Additional information on the Polymer Retrofit Coating System can be obtained from Specialty Products, Inc. at: www.specialty-products.com.

Video Vehicle Surveillance Program

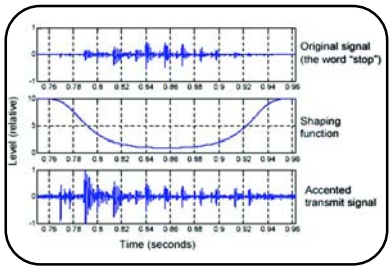
Operators viewing television or computer monitors for long periods of time often become distracted. The development and application of logical, rules-based alerting and alarming technology embedded in existing surveillance and monitoring equipment gives the operator a full-time capability to detect a potential threat and the capability to make an initial assessment of the situation. The Subgroup examined emerging state-of-the-art video systems for detecting potential vehicle bomb threats. Several manufacturers demonstrated their products, and three systems were tested in a side-by-side comparison. Two of these systems were subsequently deployed to Federal agencies for incorporation into existing security systems. Several commercial manufacturers now offer video surveillance systems that can be tailored to the specific application desired. Requests for additional information should be sent to pssubgroup@tswg.gov.

Railcar Inspection Guide and Personnel Screening Guide

Physical security and force protection personnel need consolidated guidance on how to inspect personnel or railcars for weapons, explosives, WMDs, or other hazards or contraband. These pocket-size rail inspection and personnel screening guides provide important screening information for U.S. security forces. The Railcar Inspection Guide (RIG) aids in the detection of explosive devices and other contraband by providing information on how to recognize potential threats or suspicious behavior. The Personnel Screening Guide (PSG) provides a consolidated reference for interviewing and searching individuals undergoing the screening process, including questions, warning indicators, cultural anomalies, and potential hazards. The success of the Vehicle Inspection Checklist (VIC) and Small Watercraft Inspection Guide (SWIG) spurred the development of these two new guides. The Government Printing Office currently distributes the RIG and the PSG, along with the VIC and the SWIG. Additional information about these publications can be found at the TSWG Web site: www.tswg.gov/pubs.

Vessel Identification and Positioning System

This project provided a prototype vessel identification and positioning system (VIPS) to a domestic port as well as a U.S. Naval Forces Europe (USNAVEUR) port and supported operational testing and evaluation of the systems. Each system includes multiple harbor patrol unit transponders, multiple portable transponders, patrol leader displays, a tactical operations display, and a command center base station. This effort was included in the DHS Maritime Domain Awareness Assessment conducted in June 2004 and is planned for inclusion in USNAVEUR's Critical Asset Protection System beginning in FY 2006 for 22 ports. Requests for additional information should be sent to pssubgroup@tswg.gov.



Selected Current Projects

Underwater Loudhailer

Security systems can detect swimmers and divers approaching a restricted area, but current systems have neither the range nor the clarity to warn or deter them. The Underwater Loudhailer will broadcast clear, intelligible speech to a distance of 500 yards. Its applications include deployment with harbor protection and coastal diver/swimmer detection systems, including those that are currently fielded and under development. The Loudhailer's acoustic array will compensate

for bottom and surface reflected sound waves and will broadcast in a variety of languages to alert and deter divers and swimmers approaching a restricted area. Its design also permits effective communication in deep seas, such as around oil platforms, off-shore marine terminals, and ships at anchor. The Loudhailer will be tested in FY 2005 and fielded in FY 2006.

Self-Sustaining Intrusion Detection System

Security managers seek guidance on the selection of hardware and can rarely afford to test the system in its intended environment. The Self-Sustaining Intrusion Detection Testing System is modeled on the current Underwriter's Laboratories safety test program for certifying electrical devices. Using standard protocols determined through testing, the Security Industry Association will oversee an unbiased test program to verify and certify the performance of security devices. Security managers at all levels in government and industry will be able to quickly ascertain the viability of tested equipment to perform in its intended environment, removing much of the ambiguity in selecting hardware. The initial protocols will be implemented in FY 2005 and FY 2006. Thereafter the program will be self-sustaining.

Performance Facts	
Installation	
Height	8 feet
Angle	45º below Horiz.
Detection Parameters	
Lens Type	Wide Angle
Maximum Range	30 feet (± 6 inches)
Horizontal Coverage	80º (± 2º)
Vertical Coverage	70º (± 2º)
Probability of Detection	
Across Field	
Far Field (@ 28')	0.92
Mid Range (@15')	0.99
Towards Sensor	0.95
Nuisance Alarms	
External Lighting	0 per 30 cycles
Small Animals	0 per 30 cycles
Localized Heating	2 per 30 cycles
Environmental	
Max. Operating Temp.	120º F
Min. Operating Temp.	0º F
Relative Humidity	95%

Railcar Passenger and Baggage Screening

At present, passenger and light rail systems do not employ screening procedures comparable to those used for air travel. This project will develop and integrate technologies and techniques to detect explosives and other threats. Upon completion, a prototype railroad passenger car equipped with passenger and baggage screening technologies to include bulk and trace explosives detection, metal detection, and a handheld wand for metal, plastic, and explosives detection will be delivered. The screening car will give railroad security personnel the ability to screen all passengers quickly during the boarding process. DHS plans to test a prototype of the system in FY 2005.

Drive-By Backscatter Van

Security forces and entry point screening personnel need the means to surreptitiously and remotely scan vehicles for explosives and other contraband. The Subgroup developed a utility van equipped with a backscatter X-ray imaging system to unobtrusively screen vehicles or objects of concern for explosives or other contraband. An initial prototype van underwent testing in Spring 2004. Current enhancements to the van include development of a fixed portal capability with image spatial correction and a remote operation capability. The van will also undergo upgrades to ruggedize it for environmental conditions in the field. The Backscatter Van prototype was recently evaluated and will be deployed to USNAVEUR in Fall 2004 for extended field testing.

Blast Mitigation Database

Although many blast tests have been performed in the past decade, the data from these tests are not easily accessible to engineers and planners. Aggregation of these data into a single source will help identify gaps in information and increase technical specialists' ability to extrapolate blast mitigation test data to similar situations. The database will encompass all blast mitigation final test reports authorized for release. It includes cataloging, organizing, and converting blast effect text reports and data to a common electronic format. The indexed, fully searchable database will also have an editable architecture to add new data when it becomes available, as well as an appendix containing algorithms,

formulae, and models. Planned upgrades include additional test result data and Web-based server access.

Contact Information

pssubgroup@tswg.gov

Mission

Identify, prioritize, and execute research and development projects that satisfy interagency requirements supporting intelligence gathering and special operations directed against terrorist activities.

The Surveillance, Collection, and Operations Support (SCOS) Subgroup identifies high-priority user requirements and special technology initiatives focused primarily on countering terrorism and offensive operations. The research and development projects supported by this subgroup include reducing the capabilities and support available to terrorists and enhancing U.S. capabilities to conduct retaliatory or preemptive operations. A representative from the Intelligence Community chairs the SCOS Subgroup.

Membership

Intelligence Community
U.S. Department of Defense
DIA (HUMINT, MASINT), NRO, NSA, SOCOM
U.S. Department of Homeland Security
USSS
U.S. Department of Justice
FBI

Focus Areas

The SCOS Subgroup focus areas reflect the prioritized requirements of the Intelligence Community. During FY 2004, these focus areas were:

Traditional Surveillance

Improve capabilities for the collection and enhancement of video, imagery, and audio surveillance. Success in countering terrorism often depends on the quality of intelligence collection.

Analytic Surveillance

Improve terrorist detection by developing automated tools for terrorist identification using biometrics, pattern recognition, voice and speaker recognition, and database technologies.

Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR)

Develop the means to locate, identify, and track terrorists and terrorist activities. C4ISR programs focus on developing and improving these critical abilities through programs and initiatives such as tagging, tracking, and locating (TTL); special sensors; and covert communications.

Information Operations

Exploit digital information age technology by developing and improving tools to degrade, disrupt, deny, or destroy adversary information and information systems.

Program Highlights

SCOS programs are classified or highly sensitive. Program requirements, the success of programs, and specific program capabilities cannot be discussed in an open document.

Contact Information

scossubgroup@tswg.gov

Mission

Identify, prioritize, and execute research and development projects that satisfy DoD and interagency user requirements to develop equipment and systems to support specialized force offensive operations directed against terrorist activities and groups. The use of non-sensitive prototype hardware for State and local law enforcement agencies is considered for transition and commercialization.

The Tactical Operations Support (TOS) Subgroup supports counterterrorist tactical operations, particularly those performed by specialized tactical forces trained for assault operations. The Subgroup supports technology development activities that provide a foundation for subsequent advances and the development of prototype special equipment designed to facilitate more effective execution of various tactical missions. A representative from the Department of Defense chairs the TOS Subgroup.

Membership

U.S. Department of Defense
SOCOM
U.S. Department of Energy
OS
U.S. Department of Homeland Security
USSS
U.S. Department of Justice
FBI (HRT)
U.S. Department of State
DS

Focus Areas

The TOS Subgroup focus areas reflect the prioritized requirements of offensive counterterrorism forces. During FY 2004, these focus areas were:

Advanced Imaging Systems

Develop systems that improve reduced-visibility imaging in all operating environments. The objective is to obtain the best images in reduced lighting conditions and provide systems that will enable tactical forces to operate more effectively.

Specialized Access Systems

Develop technologies that will assist tactical assault forces in accessing objectives, evaluating tactical options, and supporting efficiencies in operations, while providing added safety for personnel.

Chemical and Radiation Detectors

Develop chemical and radiological instruments that are specifically designed to support the tactical user in the field. These systems must be smaller, lighter, more robust, and more covert than conventional technologies. Development under this focus area is closely coordinated with the CBRNC subgroup.

Offensive Systems

Develop equipment and systems that will enhance the effectiveness of small offensive tactical teams in specialized operations.

Tactical Communications Systems

Develop flexible and enhanced communications capabilities to tactical forces. The major focus is on reducing the size of equipment and improving operator mobility and efficiencies.

Program Highlights

TOS programs are classified or highly sensitive. Program requirements, the success of programs, and specific program capabilities cannot be discussed in an open document.

Contact Information

tossubgroup@tswg.gov

Mission

Identify, prioritize, and execute projects that satisfy interagency requirements for the development and delivery of combating terrorism related education, training, and mission performance support products and technologies.

The Training Technology Development (TTD) Subgroup delivers training and training technologies to increase mission readiness and enhance operational capabilities in the combating terrorism community. The strategy behind the mission is to integrate and leverage Advanced Distributed Learning (ADL) technologies to deliver high-quality education and training in the medium best suited to users' needs and requirements. Representatives from the Department of Homeland Security and the Department of Defense co-chair the TTD Subgroup.

Membership

Environmental Protection Agency InterAgency Board

U.S. Department of Agriculture
APHIS

U.S. Department of Defense
JFCOM, NGB, OUSD/PR, SOCOM, USA (MANSCEN, USAR), USAF, USMC, USN

U.S. Department of Health and Human Services
FDA

U.S. Department of Homeland Security
BTS (FLETC, ODP, TSA), EPR (FEMA-USFA), IAIP, S&T (HSARPA), USCG, USSS

U.S. Department of Justice
NIJ, USMS

U.S. Department of Transportation
FRA, FTA, NHTSA

Focus Areas

The TTD Subgroup focus areas reflect the prioritized requirements of the military and civilian combating terrorism communities. During FY 2004, these focus areas were:

Advanced Distributed Learning

Develop computer-based combating terrorism training courses and the advanced tools, techniques, and guidelines required to produce them. Focus is placed on integrating computer-based delivery technologies with terrorism training materials to increase the quality, effectiveness, and accessibility of training.

Delivery Architectures

Develop new and enhance existing content and knowledge management technologies used to deliver education and training. Products target the capability to distribute on-demand, customized training to combating terrorism personnel.

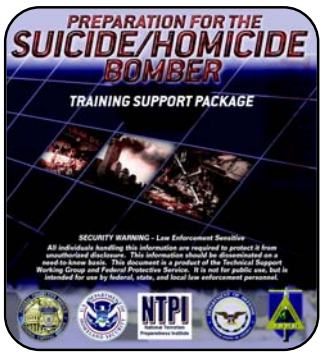
Training Aids, Devices, and Simulations

Develop training support products and virtual training environments to support mission readiness and performance. Tasks include developing training support packages for TSWG products, incorporating exercise simulations into ADL technologies, and providing simulants for training aids.

Selected Completed Projects

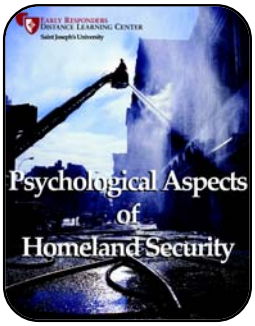
Preparation for the Suicide/Homicide Bomber Training Support Package

Developed in collaboration with the Federal Protective Service (FPS), the Preparation for the Suicide/Homicide Bomber training course guides participants through an examination of suicide bombings from a combating terrorism community perspective. The two-day course leads the student through three levels of training: Awareness Level, Operations Level, and Command Level. A few examples of topics addressed are: The Makings of a Suicide/Homicide Bombing, Proactive Countermeasures, Handling the Pre-detonation Scene, and an Overview of the National Incident Management System. The Training Support Package includes an instructor manual, student manual, video support segments, and a train-the-trainer video. Requests for additional information should be sent to ttdsubgroup@tswg.gov.



Small Watercraft Inspection Guide Training Support Package

Security forces and other Federal agencies will benefit from a systematic approach for screening vessels for improvised explosives and other contraband. The Physical Security Subgroup at TSWG developed a pocket-sized reference guide that provides information on searching compartments of a vessel for WMDs and explosives. Due to overwhelming interest in the Small Watercraft Inspection Guide (SWIG), a complete training support package was developed for use by government emergency response teams and law enforcement officers. The SWIG Training Support Package is procurement-ready for DoD and other government agencies. Product and procurement information can be obtained from: www.tswg.gov/tswg/prods_pubs/SWIG_TSP.htm.



Psychological Aspects of WMDs/Terrorism

One of the greatest challenges facing senior leadership, response personnel, and health professionals is coping with the disorientation, fear, anger, grief, and terror caused by WMD incidents. This project provides a training program focused on recognizing, minimizing, and managing the severe psychological stress associated with WMD and terrorism incidents. The six-module training program focuses on critical issues surrounding the psychological impacts and effects of terrorism and decontamination, panic response operations, risk communication and management, and mental health interventions. The courses are currently available through the developer, Saint Joseph's University's Early Responders Distance Learning Center, in Web-based, CD-ROM, and classroom delivery formats. Course information is available at: http://erdlc.sju.edu/education-course.php?group_id=7.

CJTF-7 OIF Smart Book

Military personnel need immediate access to mission planning and execution data. The CJTF-7 OIF (Combined Joint Task Force, Operation Iraqi Freedom) Smart Book provides tactics, techniques, procedures, and best practices on the following topics: Convoy Operations (combat and non-combat), Vehicle Search Techniques, Improvised Explosive Device (IED) threats, Vehicle Bomb IED threats, and IED procedures. The smart book reflects CJTF-7 Standard Operating Procedure and has been delivered to OIF. Requests for additional information should be sent to ttdsubgroup@tswg.gov.

Selected Current Projects

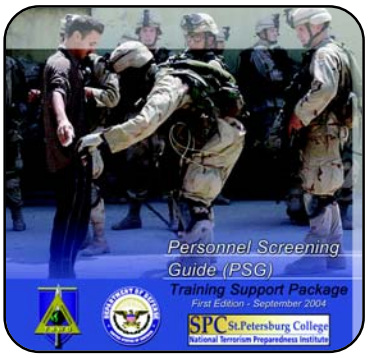
Scenario-Based Interactive Exercise Simulation

Within the combating terrorism community, there is a need to provide technology solutions to maximize training to a large, geographically dispersed community while reducing travel and training costs. This project will design and develop scenario-based, interactive exercise simulation to complement existing table top, command post, and full-scale CBRNE incident response training and exercise programs. This technology will provide a multi-player, on-line gaming technology that incorporates virtual reality technologies and interactive simulation with the visual appeal of gaming environments. The scenarios will be role-based and will focus on familiarizing role players with agency roles, assets, and response protocols.

Rapid Education for Medical Professionals

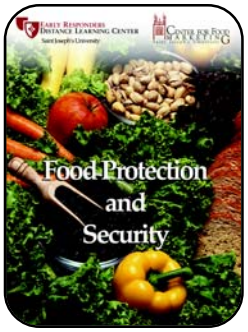
Medical professionals require timely delivery of alerts and relevant education to effectively respond to a terrorist event. The Alert and Education Tool for Medical Professionals will provide the most current treatments and procedures for chemical, biological, and radiological threat agents. The automated, Internet-based tool will disseminate educational resources to Federal, State, and local health agencies.

Personnel Screening Guide Training Support Package



Since 9/11, security has been heightened at many major gatherings, targets of high symbolic value, and at overseas facilities and installations. The security checkpoint has been the primary screening method used at these sites by military and civilian security personnel. The one-day Personnel Screening Guide (PSG) Training Support Package (TSP) provides training on identifying suspicious individuals, completing a proper interview, and conducting searches on both individuals and personal belongings. Under simultaneous development, the Railcar Inspection Guide (RIG) TSP will guide participants in conducting security operations at rail facilities and implementing specific methodologies for searching railcars and their occupants. The PSG and RIG were developed by the Physical Security Subgroup at TSWG.

Food Protection and Security Training for Critical and Overseas Facilities



Food is a widespread medium for delivering potential terrorist threats. This training package teaches food management and terrorism response personnel to recognize, minimize, and manage the threat of terrorist activities across the supply chain from farm to table. Phase I of the project is complete and contains five modules: Introduction to Food Security and Terrorism, Food Security Risk Assessment, Food Security Risk Communication, Food Security Risk Management, and Food Supply Chain Traceability. Phase II of the project is underway and will include three modules: Introduction to Food Security Law, Securing our Global Food Supply, and Leadership in Times of Crisis.

Management of Agricultural Terrorism

A deliberately induced large-scale animal disease outbreak such as foot and mouth disease would challenge the response resources of the United States. It is crucial that an immediate and appropriate response be initiated at the time of detection to minimize its impact. This six module training program addresses: Introduction to Animal Health Emergency Management; Principles of the Incident Command System; Introduction to Agriculture and its Industries; Animal Pathogens – Pathways of Introduction, Disease Recognition, Reporting and Awareness; Disease Response Mechanisms and Bio-security; and Recovery – Animal Support Response. Anchoring themes in each module will be communication, coordination, and functional roles at the Federal, State and local levels.

Contact Information

ttdsubgroup@tswg.gov

Mission

To identify, prioritize, and execute research and development projects that satisfy interagency requirements for equipment and systems that alert and prevent attacks on VIP protectees. This includes hardware and tools that provide security to both the VIPs and their protectors. Inherent in this development is additional emphasis on life safety and emergency response equipment.

The VIP Protection (VIP) Subgroup focuses on the development of prototype hardware, systems, personnel protection equipment, and diagnostic and reference tools and standards that will support greater security for VIPs. To be effective, personnel who are charged with the safety of these VIPs must also have protective equipment that will prevent injury and tools that will improve their effectiveness. These developments benefit the operational effectiveness of Federal, State, military, and local law enforcement personnel who are charged with the protection of VIPs. These technologies and tools also have application to protection of law enforcement and military personnel who engage in hazardous combat-like environments. The VIP Protection Subgroup is chaired by a representative from the U.S. Secret Service.

Membership

U.S. Capitol Police
U.S. Department of Commerce
NIST (OLES)
U.S. Department of Defense
USA (Natick RD&E Center, TACOM), USN (SWC)
U.S. Department of Energy
OS
U.S. Department of Homeland Security
USSS (SSD, TSD)
U.S. Department of Justice
NIJ
U.S. Department of State
DS

Focus Areas

The VIP Subgroup focus areas reflect the prioritized requirements of the personnel protection community. During FY 2004, these focus areas were:

Vehicle Protection and Performance

Improve the safety and effectiveness of armored vehicles to protect passengers. This includes the development of upgrades to vehicle systems that will enhance the performance and reliability of the vehicles in a broad range of operational environments. It also supports the validation of the existing designs against specific threats.

Transparent Armor Development

Develop and validate tools that will predict performance and support advanced design of transparent armor. This includes evaluations and designs that will protect against a broad range of threat projectiles. Because of the significant weight penalty of transparent armor, this area also focuses on the development of advanced lightweight transparent armor that will provide substantial reduction of the weight and thickness necessary to obtain the required protection.

Individual Protection Systems

Develop and improve personal body armor and methods for the protection of personnel assigned to VIP details. Many of the developments will also support the protection of law enforcement officers. This focus area emphasizes improving the performance of body armor, understanding its limitations (e.g., ballistic and thermal), and providing associated systems that will improve the comfort and effectiveness for the wearer. It also includes technologies that identify situations where protection personnel and the VIPs under their protection are in need of support or assistance.

Emerging Threats

Develop methods and systems that will identify, prevent, or defeat potential attacks from remote areas. This includes technologies that will identify potential

sniper or remote attacks and will alert users. The technologies will provide locating information and develop appropriate countermeasures.

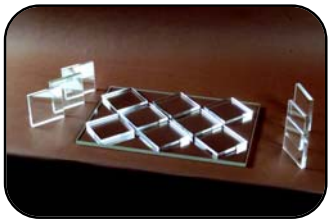
VIP Installation Protection

Develop threat identification and warning technologies for potential threats directed against critical installations occupied by senior government officials. Included are appropriate countermeasures that will enhance the safety of the installations during terrorist actions.

Selected Completed Projects

Lightweight Vehicle Armor

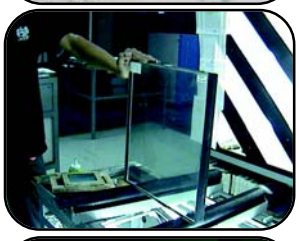
The lightweight vehicle armor program focused on providing suitable protection to counter the highly effective armor-piercing projectiles. The project developed an effective armor that could be installed in typical armored passenger vehicles. The armor has demonstrated effectiveness against both 7.62 and 5.56 rounds. This armor configuration will be considered for application to selected armored limousines.

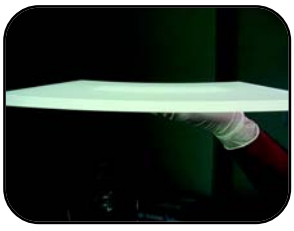


Multi-Hit ALON Testing

Researchers proved that aluminum-oxynitride (ALON), a transparent armor ceramic, can provide ballistic protection equivalent to standard glass armor with reduced weight and thickness in a laboratory setting. Specifically, ALON can provide superb multi-hit protection at approximately half the weight of conventional transparent armor. This testing will support a follow-on task demonstrating the practicality of installing full-size ALON windows into a commercial vehicle.

Selected Current Projects





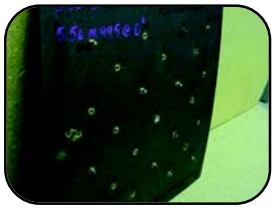
Transparent Armor Developments

The VIP Subgroup is investigating the next generation of transparent armor through the development of a design model for predicting the performance of these types of armor. This model is currently being validated against the results of actual ballistics testing. Results from the validation testing will be incorporated into the model. Once completed, the design model will offer a more cost-effective approach to designing transparent armor.

An important goal of transparent armor development is reducing the overall weight and thickness of the armor without reducing its protective properties. Two armors under development that will accomplish this goal are ALON and Spinel. ALON has already been proven to offer a high level of multi-hit protection. In order to demonstrate that ALON is operationally feasible and cost-effective, the Surmet Corporation is fabricating a window set for a Ford F-250 pickup truck. This project will allow users to evaluate the durability of ALON over time.

Spinel transparent armor is being developed as an alternative to ALON. While still in the early stages of development, an on-going project is demonstrating the ability to manufacture the armor in large pieces. Manufacturing transparent armor in large pieces is critical to making the product cost-effective. Producing large pieces will also allow users to conduct comparison testing between the two armors in terms of cost, performance, and durability.

Multi-Hit Test Standard



The Multi-Hit Test Standard provides a consistent procedure for subjecting body armor to the dynamic effects of being hit with multiple shots in a short time frame. The project developed a computer-controlled test system that allows for repeatable shot spacing and timing. This project will further evaluate more advanced methods to measure the backface deformation, a metric used to assess body armor effectiveness.

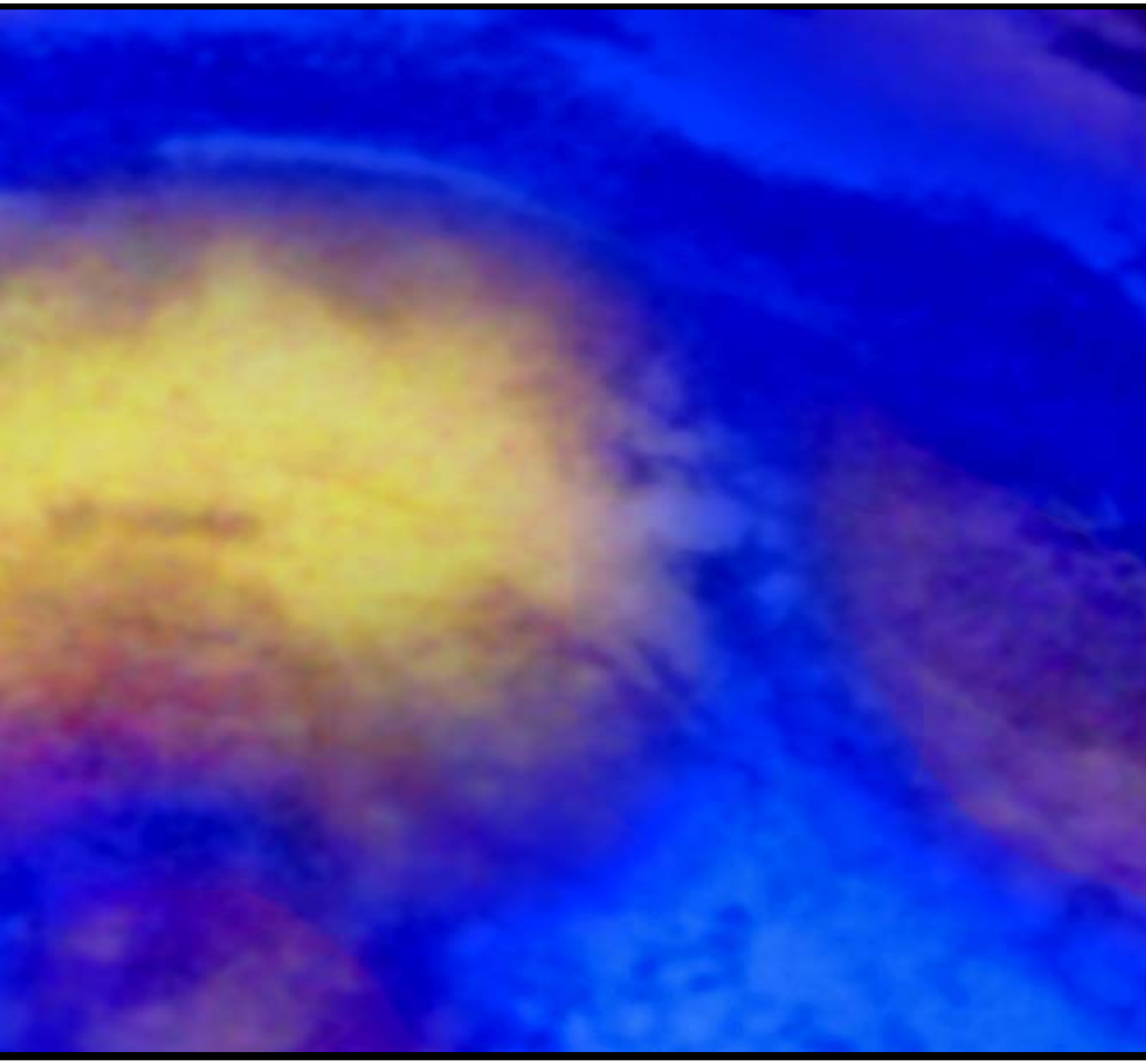
Armored Passenger Vehicle Standards

Currently, no comprehensive standard exists that prescribes the performance criteria for armored passenger vehicles (APVs). The absence of reliable standards makes evaluating APVs difficult for procurement personnel. The Subgroup is developing performance standards in five key component areas: ballistic protection, blast protection, optical performance of transparent armor, overall automotive performance, and quality control. As performance criteria in each field are established, the information will be compiled into one comprehensive standard. This standard will allow users in the VIP protection field to better understand the capabilities of currently available APVs.

Contact Information

vipsubgroup@tswg.gov

APPENDICES



BAA Information Delivery System (BIDS)

TSWG seeks technology solutions that address operational and technological shortfalls identified by Government agency users at least once annually. User requirements are disclosed in a solicitation format called a Broad Agency Announcement (BAA). The BAA enables the Government to solicit industry, academia, and Government laboratories for innovative research and development solutions to these requirements. The BAA is advertised in the Federal Business Opportunities at: www.fedbizopps.gov. The FedBizOpps site directs interested bidders to the appropriate Web address where additional information for submitting a proposal is posted. Each open BAA is also posted on the TSWG Web site at: www.bids.tswg.gov. At this site, the BAA Information Delivery System (BIDS) provides an electronic submission and record evaluation capability for receiving and evaluating responses to a BAA. BIDS is a secure 128-bit encryption connection that provides proposal response uploads for prospective bidders and ensures control of bidder proprietary data.

In addition, TSWG has released BAAs for the Department of Homeland Security. By harnessing the technical capabilities of BIDS to support Government initiatives, TSWG increases the return on investment in combating terrorism technologies made by multiple Federal agencies. The BIDS system has proved capable of handling larges volumes of proposals. In 2001 alone the system processed nearly 17,000 submissions. BIDS continues to serve as a model for other Federal programs that seek to solicit technical proposals while eliminating the inconvenience of paper forms, the unnecessary waste in processing time, and excessive proposal mailing expenses.

Appendices

TSWG Membership

Executive Branch

U.S. Department of Defense

- Armed Forces Institute of Pathology
- Defense Advanced Research Projects Agency
- Defense Computer Forensics Laboratory
- Defense Intelligence Agency
  - Central MASINT Organization
  - Defense HUMINT Service
- Defense Protective Service
- Defense Threat Reduction Agency
- Joint Chiefs of Staff
- National Guard Bureau
- National Reconnaissance Office
- National Security Agency
- Office of the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict
- Office of the Deputy Assistant to the Secretary of Defense for Chemical and Biological Defense
- Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics
- Office of the Under Secretary of Defense for Personnel and Readiness
- Pentagon Force Protection Agency
- Polygraph Institute
- U.S. Air Force
  - Air Combat Command
  - Air Force Research Lab
  - Electronic Systems Center
  - Force Protection Battle Lab
  - Office of Special Investigations
  - Surgeon General
- U.S. Army
  - 52nd Ordnance Group
  - Chemical School
  - Corps of Engineers
  - Criminal Investigation Command
  - Forces Command
  - Maneuver Support Center
  - Medical Research Institute of Infectious Diseases
  - Natick Research, Development, and Engineering Center
  - National Ground Intelligence Center
  - Soldier and Biological Chemical Command
    - Edgewood Chemical Biological Center
  - Tank-Automotive and Armaments Command
  - Technical Escort Unit
  - U.S. Army Reserve
- U.S. Central Command
- U.S. European Command
- U.S. Joint Forces Command
- U.S. Marine Corps
  - Chemical Biological Incident Response Force
  - Critical Infrastructure Protection

- U.S. Navy
  - Joint Program Office, Special Technology Countermeasures
  - Naval Air Warfare Center
  - Naval Criminal Investigative Service
  - Naval Explosive Ordnance Disposal Technology Division
  - Naval Forces Central Command
  - Naval Research Laboratory
  - Naval Surface Warfare Center
- U.S. Special Operations Command

Environmental Protection Agency

- Criminal Investigation Division
- National Enforcement Investigations Center
- National Homeland Security Research Center
- Office of Ground Water and Drinking Water

Federal Reserve Board

General Services Administration

- Mail Policy

Intelligence Community

InterAgency Board

National Aeronautics and Space Administration

National Transportation Safety Board

Nuclear Regulatory Commission

U.S. Department of Agriculture

- Agricultural Research Service
- Animal and Plant Health Inspection Service
- Food Safety and Inspection Service
- Forest Service

U.S. Department of Commerce

- National Institute of Standards and Technology
  - Office of Law Enforcement Standards

U.S. Department of Energy

- National Nuclear Security Administration
- Office of Energy Assurance
- Office of Security

U.S. Department of Health and Human Services

- Centers for Disease Control and Prevention
- Food and Drug Administration
- National Institute for Occupational Safety and Health

U.S. Department of Homeland Security

- Border and Transportation Security Directorate
  - Bureau of Customs and Border Protection
  - Federal Law Enforcement Training Center
  - Immigration and Customs Enforcement
    - Federal Air Marshal Service
    - Federal Protective Service
    - Forensic Document Laboratory

  - Office for Domestic Preparedness
  - Transportation Security Administration
- Emergency Preparedness and Response Directorate
  - Federal Emergency Management Agency
    - U.S. Fire Administration
- Information Analysis and Infrastructure Protection Directorate
  - National Infrastructure Protection Center
- Science and Technology Directorate
  - Homeland Security Advanced Research Projects Agency
- U.S. Coast Guard
- U.S. Secret Service
  - Special Services Division
  - Technical Security Division

U.S. Department of Justice

- Bureau of Alcohol, Tobacco, Firearms, and Explosives
- Drug Enforcement Administration
- Federal Bureau of Investigation
  - Bomb Data Center
  - Hazardous Materials Response Unit
  - Hostage Rescue Team
  - Weapons of Mass Destruction Operations Unit
- Federal Bureau of Prisons
- National Institute of Justice
  - National Center for Forensic Science
  - National Forensic Science Technology Center
- Office of Justice Programs
- U.S. Marshals Service

U.S. Department of State

- Bureau of Diplomatic Security
- Office of the Coordinator for Counterterrorism
- Overseas Building Operations

U.S. Department of Transportation

- Federal Aviation Administration
- Federal Railroad Administration
- Federal Transit Administration
- Intelligence and Security
- National Highway Traffic Safety Administration
- Office of Information Services
- Volpe National Transportation Systems Center

U.S. Postal Service

- U.S. Postal Inspection Service

Judicial Branch

Supreme Court of the United States

Legislative Branch

U.S. Capitol Police

U.S. Senate

- Sergeant at Arms

State and Local Agencies

Fairfax County (VA) Police Department

Fire Department, City of New York

National Bomb Squad Commanders Advisory Board

- Bloomington, Minnesota Police Department (Northern region)
- Houston, Texas Police Department (Southern region)
- Los Angeles, California Police Department (Western region)
- Philadelphia, Pennsylvania Police Department (Eastern region)

Port Authority of New York/New Jersey

Washington Metropolitan Area Transit Authority

TSWG Subgroup Membership

Chemical, Biological, Radiological, and Nuclear Countermeasures

Environmental Protection Agency

Fire Department, City of New York

General Services Administration

- Mail Policy

Intelligence Community

InterAgency Board

Nuclear Regulatory Commission

U.S. Capitol Police

U.S. Department of Agriculture

- Agricultural Research Service
- Animal and Plant Health Inspection Service
- Food Safety and Inspection Service

U.S. Department of Commerce

- National Institute of Standards and Technology

U.S. Department of Defense

- Defense Intelligence Agency
- Defense Protective Service
- Defense Threat Reduction Agency
- Joint Chiefs of Staff
- National Security Agency
- Office of the Deputy Assistant to the Secretary of Defense for Chemical and Biological Defense
- Pentagon Force Protection Agency
- U.S. Air Force
  - Air Combat Command
  - Electronic Systems Center
  - Force Protection Battle Lab
  - Surgeon General
- U.S. Army
  - 52nd Ordnance Group
  - Chemical School
  - Forces Command
  - Maneuver Support Center
  - Medical Research Institute of Infectious Diseases
  - National Ground Intelligence Center
  - Soldier and Biological Chemical Command
    - Edgewood Chemical Biological Center
  - Technical Escort Unit
- U.S. Marine Corps
  - Chemical Biological Incident Response Force
- U.S. Navy
  - Naval Air Warfare Center
  - Naval Forces Central Command
  - Naval Surface Warfare Center
- U.S. Special Operations Command

U.S. Department of Energy

- Office of Security

U.S. Department of Health and Human Services

- Centers for Disease Control and Prevention
- Food and Drug Administration
- National Institute for Occupational Safety and Health

U.S. Department of Homeland Security

- Border and Transportation Security Directorate
  – Transportation Security Administration
- Emergency Preparedness and Response Directorate
  – Federal Emergency Management Agency
- Science and Technology Directorate
  – Homeland Security Advanced Research Projects Agency
- U.S. Coast Guard
- U.S. Secret Service
  – Technical Security Division

U.S. Department of Justice

- Federal Bureau of Investigation
  – Bomb Data Center
  – Hazardous Materials Response Unit
  – Weapons of Mass Destruction Operations Unit
- National Institute of Justice
- Office of Justice Programs
- U.S. Marshals Service

U.S. Department of State

- Bureau of Diplomatic Security
- Office of the Coordinator for Counterterrorism
- Overseas Building Operations

U.S. Department of Transportation

- Intelligence and Security

U.S. Postal Service

- U.S. Postal Inspection Service

U.S. Senate

- Sergeant at Arms

Washington Metropolitan Area Transit Authority

Explosives Detection

U.S. Capitol Police

U.S. Department of Defense

- Defense Intelligence Agency
- National Security Agency
- U.S. Air Force
  – Air Combat Command
  – Air Force Research Lab
  – Electronic Systems Center

- U.S. Army
  - Technical Escort Unit
- U.S. Navy
  - Naval Criminal Investigative Service
  - Naval Explosive Ordnance Disposal Technology Division
  - Naval Research Laboratory

U.S. Department of Energy
- Office of Security

U.S. Department of Homeland Security
- Border and Transportation Security Directorate
  - Bureau of Customs and Border Protection
  - Immigration and Customs Enforcement
    - Federal Air Marshal Service
    - Federal Protective Service
- Emergency Preparedness and Response Directorate
  - Transportation Security Administration
- Science and Technology Directorate
  - Homeland Security Advanced Research Projects Agency
- U.S. Coast Guard
- U.S. Secret Service

U.S. Department of Justice
- Bureau of Alcohol, Tobacco, Firearms, and Explosives
- National Institute of Justice

U.S. Department of State
- Bureau of Diplomatic Security

U.S. Postal Service
- U.S. Postal Inspection Service

Improvised Device Defeat

Fairfax County (VA) Police Department

Intelligence Community

National Bomb Squad Commanders Advisory Board

Bloomington, Minnesota Police Department (Northern region)
Houston, Texas Police Department (Southern region)
Los Angeles, California Police Department (Western region)
Philadelphia, Pennsylvania Police Department (Eastern region)

U.S. Capitol Police

U.S. Department of Defense
- U.S. Air Force
- U.S. Army
- U.S. Marine Corps
- U.S. Navy

U.S. Department of Homeland Security
- Border and Transportation Security Directorate
  - Office for Domestic Preparedness
  - Transportation Security Administration

- Information Analysis and Infrastructure Protection Directorate
- U.S. Secret Service

U.S. Department of Justice

- Bureau of Alcohol, Tobacco, Firearms, and Explosives
- Federal Bureau of Investigation
- National Institute of Justice
- U.S. Marshals Service

Infrastructure Protection

Environmental Protection Agency

Nuclear Regulatory Commission

U.S. Department of Agriculture

- Forest Service

U.S. Department of Commerce

- National Institute of Standards and Technology

U.S. Department of Defense

- Defense Threat Reduction Agency
- U.S. Air Force
  – Office of Special Investigations
- U.S. Army
  – Corps of Engineers
- U.S. Marine Corps
  – Critical Infrastructure Protection
- U.S. Navy
  – Joint Program Office, Special Technology Countermeasures
  – Naval Criminal Investigative Service
  – Naval Surface Warfare Center

U.S. Department of Energy

- Office of Energy Assurance
- Office of Security

U.S. Department of Homeland Security

- Emergency Preparedness and Response Directorate
  – Federal Emergency Management Agency
- Border and Transportation Security Directorate
  – Immigration and Customs Enforcement
    – Federal Protective Service
  – Office for Domestic Preparedness
  – Transportation Security Administration
- Information Analysis and Infrastructure Protection Directorate
  – National Infrastructure Protection Center
- Science and Technology Directorate
  – Homeland Security Advanced Research Projects Agency
- U.S. Secret Service

U.S. Department of Justice

- Federal Bureau of Investigation

U.S. Department of Transportation
- Federal Aviation Administration
- Volpe National Transportation Systems Center

Investigative Support and Forensics

Environmental Protection Agency
- Criminal Investigation Division
- National Enforcement Investigations Center

Federal Reserve Board

Intelligence Community

National Transportation Safety Board

U.S. Department of Commerce
- National Institute of Standards and Technology
  – Office of Law Enforcement Standards

U.S. Department of Defense
- Armed Forces Institute of Pathology
- Defense Advanced Research Projects Agency
- Defense Computer Forensics Laboratory
- Defense Threat Reduction Agency
- National Security Agency
- Polygraph Institute
- U.S. Air Force
  – Office of Special Investigations
- U.S. Army
  – Criminal Investigation Command
- U.S. Marine Corps
  – Chemical Biological Incident Response Force
- U.S. Navy
  – Naval Criminal Investigative Service

U.S. Department of Energy
- Office of Security

U.S. Department of Homeland Security
- Border and Transportation Security Directorate
  – Bureau of Customs and Border Protection
  – Immigration and Customs Enforcement
    – Federal Protective Service
    – Forensic Document Laboratory
  – Transportation Security Administration
- Emergency Preparedness and Response Directorate
  – Federal Emergency Management Agency
- U.S. Secret Service

U.S. Department of Justice
- Bureau of Alcohol, Tobacco, Firearms, and Explosives
- Drug Enforcement Administration
- Federal Bureau of Investigation
- National Institute of Justice
  – National Center for Forensic Science

  - National Forensic Science Technology Center
- U.S. Marshals Service

U.S. Department of Transportation

- Federal Aviation Administration

U.S. Postal Service

- U.S. Postal Inspection Service

Physical Security

Federal Reserve Board

Intelligence Community

National Aeronautics and Space Administration

Nuclear Regulatory Commission

Port Authority of New York/New Jersey

Supreme Court of the United States

U.S. Department of Defense

- Defense Threat Reduction Agency
- Joint Chiefs of Staff
- National Security Agency
- Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics
- U.S. Air Force
- U.S. Army
- U.S. Central Command
- U.S. European Command
- U.S. Joint Forces Command
- U.S. Marine Corps
- U.S. Navy

U.S. Department of Energy

- National Nuclear Security Administration
- Office of Security

U.S. Department of Homeland Security

- Border and Transportation Security Directorate
  - Bureau of Customs and Border Protection
  - Federal Law Enforcement Training Center
  - Transportation Security Administration
    - Office of Maritime & Land Security
- U.S. Coast Guard
- U.S. Secret Service

U.S. Department of Justice

- Bureau of Alcohol, Tobacco, Firearms, and Explosives
- Federal Bureau of Prisons
- National Institute of Justice

U.S. Department of State

- Bureau of Diplomatic Security

U.S. Department of Transportation

- Office of Information Services

U.S. Postal Service

- U.S. Postal Inspection Service

Surveillance, Collection, and Operations Support

Intelligence Community

U.S. Department of Defense

- Defense Intelligence Agency
  - Central MASINT Organization
  - Defense HUMINT Service
- National Reconnaissance Office
- National Security Agency
- U.S. Special Operations Command

U.S. Department of Homeland Security

- U.S. Secret Service

U.S. Department of Justice

- Federal Bureau of Investigation

Tactical Operations Support

U.S. Department of Defense

- U.S. Special Operations Command

U.S. Department of Energy

- Office of Security

U.S. Department of Homeland Security

- U.S. Secret Service

U.S. Department of Justice

- Federal Bureau of Investigation
  - Hostage Rescue Team

U.S. Department of State

- Bureau of Diplomatic Security

Training Technology Development

Environmental Protection Agency

InterAgency Board

U.S. Department of Agriculture

- Animal and Plant Health Inspection Service

U.S. Department of Defense

- National Guard Bureau
- Office of the Under Secretary of Defense for Personnel and Readiness
- U.S. Air Force
- U.S. Army
  - Maneuver Support Center
  - U.S. Army Reserve
- U.S. Joint Forces Command

- U.S. Marine Corps
- U.S. Navy

U.S. Department of Health and Human Services

- Food and Drug Administration

U.S. Department of Homeland Security

- Border and Transportation Security Directorate
  - Federal Law Enforcement Training Center
  - Office for Domestic Preparedness
  - Transportation Security Administration
- Emergency Preparedness & Response Directorate
  - Federal Emergency Management Agency
    - U.S. Fire Administration
- Information Analysis and Infrastructure Protection Directorate
- Science and Technology Directorate
- U.S. Coast Guard
- U.S. Secret Service

U.S. Department of Justice

- National Institute of Justice
- U.S. Marshals Service

U.S. Department of Transportation

- Federal Railroad Administration
- Federal Transit Administration
- National Highway Traffic Safety Administration

VIP Protection

U.S. Capitol Police

U.S. Department of Commerce

- National Institute of Standards and Technology
  - Office of Law Enforcement Standards

U.S. Department of Defense

- U.S. Army
  - Natick Research, Development, and Engineering Center
  - Tank-Automotive and Armaments Command

U.S. Department of Energy

- Office of Security

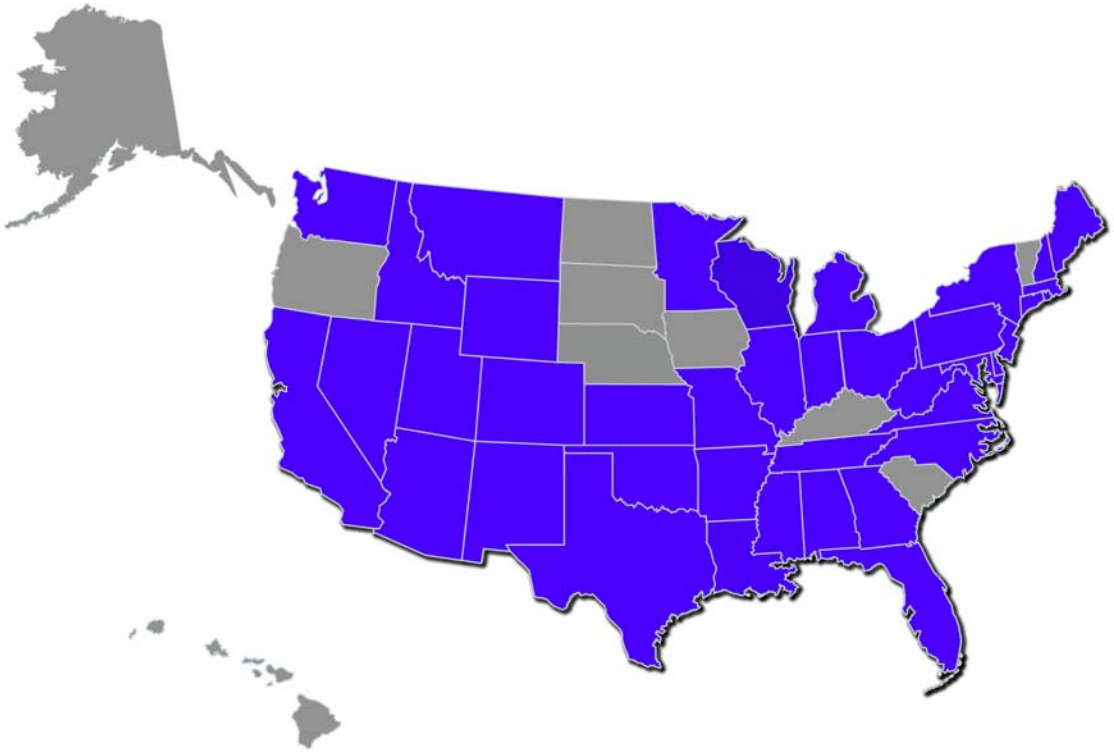
U.S. Department of Homeland Security

- U.S. Secret Service
  - Special Services Division
  - Technical Security Division

U.S. Department of State

- Bureau of Diplomatic Security

TSWG Performers



Alabama

Auburn University, Auburn
Photon-X, Huntsville
University of Alabama at Birmingham

Arizona

Authenti-Corp, Gilbert
Litton Systems, Inc., EOS Division, Tempe
Pacific Scientific, Chandler

Arkansas

The Tekne Group, Inc., Hot Springs
University of Arkansas at Fayetteville

California

3rd Ring, Mammoth Lakes
Advanced Countermeasures Systems, Rancho Cordova
Ancore, Santa Clara
ComGlobal Systems, Inc., San Diego
Delphi, San Diego
Dynamics Technology, Inc., Torrance
Intelligent Optical Systems, Inc., Torrance
Jet Propulsion Laboratory, Pasadena
Lawrence Berkeley National Laboratory, Berkeley

Lawrence Livermore National Laboratory, Livermore
Naval Air Warfare Station, Point Mugu
Quantum Magnetics, Inc., San Diego
Rapiscan Security Products, Hawthorne
Raymat Materials, Fremont
Raytheon Company, Electronic Systems, Buena Park
Raytheon Company NCS, El Segundo
Safe Environment Engineering, Valencia
San Jose State University, San Jose
Science Applications International Corporation, San Diego
Smiths Detection, Pasadena
Space and Naval Warfare Systems Command, San Diego
Special Technologies Laboratory, Santa Barbara
SRI International, Menlo Park
Tactical Survey Group, Inc., Crestline
University of California at Davis
University of California at San Diego
WaveBand Corporation, Irvine
WFI Government Services, San Diego
X-Ray Instrumentation Associates, Newark

Colorado

Applied Research Associates, Inc., Littleton
Colorado State University, Fort Collins
Thermo MF Physics, Colorado Springs

Connecticut

Applied Physical Sciences Corporation, New London
Interspiro, Inc., Branford
Nextgen Fiber Optics, LLC, Dayville
Pulmatrix, Inc., Ridgefield
United Technologies Research Center, Hartford

Delaware

DuPont, Wilmington

District of Columbia

International Association of Firefighters
Psynapse
U.S. Naval Research Laboratory

Florida

46 Test Squadron, Eglin Air Force Base
Applied Research Associates, Tyndall Air Force Base
Engineering Technology, Inc., Orlando
Gemini Industries, Tampa
Harris Government Communications Systems Division, Melbourne
Knights Armaments Company, Vero Beach
Media Management Group, Inc., Clearwater
National Center for Forensic Science, Orlando

Purified MicroEnvironments, Ormond Beach
St. Petersburg College, National Terrorism Preparedness Institute, St. Petersburg
Tampa Armature Works, Inc., Jacksonville
U.S. Air Force Research Laboratory, Tyndall Air Force Base

Georgia

Emory University, Atlanta
Georgia Tech Research Institute, Atlanta

Idaho

Idaho National Engineering and Environmental Laboratory, Idaho Falls

Illinois

Argonne National Laboratory, Argonne
Gas Technology Institute, Des Plaines
Nanosphere, Inc., Northbrook

Indiana

U.S. Naval Surface Warfare Center, Crane Division

Kansas

Kansas State University, Manhattan

Louisiana

Louisiana State University, Baton Rouge

Maine

Sensor Research and Development Corporation, Orono

Maryland

20/20 Gene Systems, Rockville
Advanced Engineering & Sciences, Annapolis Junction
Armed Forces Radiobiology Research Institute, Bethesda
Eagan, McAllister Associates, Inc., Lexington Park
GEOMET Technologies, Inc., Germantown
Jackson and Tull, Seabrook
Johns Hopkins University Applied Physics Laboratory, Laurel
Johns Hopkins University School of Medicine, Baltimore
Lagus Applied Technology, Olney
Multispectral Solutions, Inc., Germantown
Naval Explosive Ordnance Disposal Technology Division, Indian Head
Syntonics, Ellicott City
Sytex, Inc., Ellicott City
Technology Assessment & Transfer, Inc., Annapolis
Techno-Sciences Inc., Lanham
The Windermere Group, LLC, Annapolis
U.S. Army, Edgewood Chemical Biological Center, Aberdeen Proving Ground
U.S. Department of Commerce, National Institute of Standards and Technology, Gaithersburg
U.S. Navy, Naval Air Warfare Center Aircraft Division, Patuxent River
U.S. Navy, Naval Surface Warfare Center, Carderock
Veritas, Inc., Rockville

Massachusetts

American Science & Engineering, Billerica
BBN Technologies, Cambridge
Cell Exchange, Inc., Cambridge
CyTerra Corporation, Waltham
Foster-Miller, Inc., Waltham
GE Ion Track, Wilmington
iRobot Corporation, Burlington
Massachusetts General Hospital, Boston
Massachusetts Institute of Technology, Cambridge
Massachusetts Institute of Technology, Lincoln Laboratory, Lexington
Millivision, Inc., South Deerfield
Pulmatrix, Inc., Cambridge
SenTech, Inc., Stoneham
Surmet Corp., Burlington
Technical Products, Inc., Framingham
The Charles Stark Draper Laboratory, Inc., Cambridge
TIAX, LLC, Cambridge
Tufts University, Medford
U.S. Army, Natick RD&E Center, Natick
U.S. Department of Transportation, Volpe National Transportation Systems Center, Cambridge
University of Massachusetts at Amherst
Viisage Technology, Inc., Littleton
Woods Hole Oceanographic Institution, Woods Hole

Michigan

Michigan State University, East Lansing
Picometrix, Inc., Ann Arbor

Minnesota

Honeywell Laboratories, Minneapolis
The Mayo Clinic, Rochester
University of Minnesota at Duluth
University of Minnesota at Minneapolis

Mississippi

Mississippi State University at Starkville
ProVision Technologies, Stennis Space Center

Missouri

Clean Earth Technologies, LLC, Earth City
Hanford Nuclear Services, Inc., West Plains
Midwest Research Institute, Kansas City
Washington University, St. Louis

Montana

Veridical Research and Design, Bozeman

Nevada

Remote Sensing Laboratory of Bechtel, Las Vegas
University of Nevada at Las Vegas
Varian, Inc., Las Vegas

New Hampshire

BAE Systems (IEWS), Nashua
Dartmouth University, Hanover
DTC Communications Inc., Nashua
Global Manufacturing Company, Pittsfield
Impact Science and Technology, Hollis

New Jersey

Composecure, LLC, Mountainside
FibreGuide, Stirling
Hi Temp Technology, Inc., Flemmington
JeBen Photonics, Inc., Denville
JP Laboratories, Middlesex
New Jersey Institute of Technology, Newark
Rutgers University, Piscataway
Sarnoff Corporation, Princeton
Structured Materials Industries, Piscataway
U.S. Army Communications-Electronics Command, Fort Monmouth

New Mexico

Applied Research Associates, Inc., Albuquerque
Intellite, Inc., Albuquerque
Los Alamos National Laboratory, Los Alamos
MesoSystems Technology, Inc., Albuquerque
National Assessment Group, Albuquerque
New Mexico Institute of Mining and Technology, Energetic Materials Research and Testing Center, Socorro
Sandia National Laboratories, Albuquerque
Science and Engineering Associates, Inc., Albuquerque

New York

Calspan-UB Research Center, Inc., Buffalo
Esensors, Inc., Amherst
GE Global Research, Niskayuna
IBM, Watson Research Center, Yorktown Heights
New York University, New York
Northrop Grumman Corporation, Buffalo
Northrop Grumman ISS, Bethpage
Portable Environments, LLC, Ithaca
Rensselaer Polytechnic Institute, Troy
Sensatex, Inc., New York
Sentigen Holding Corporation, New York
State University of New York at Buffalo
U.S. Air Force Research Laboratory, Rome

North Carolina

North Carolina State University, Textile Protection and Comfort Center, Raleigh
Research Triangle Institute, Research Triangle Park
Signalscape, Inc., Raleigh

Ohio

Air Force Institute of Technology, Wright-Patterson Air Force Base
Battelle Memorial Institute, Columbus
Komar Industries, Inc., Groveport
MTL Systems, Inc., Dayton
NAIC, Wright-Patterson Air Force Base
Northeastern Ohio Universities College of Medicine, Rootstown
Ohio University, Clippinger Laboratories, Athens
Total Fire Group/Morning Pride Manufacturing, Dayton
University of Dayton Research Institute, Dayton

Oklahoma

Nomadics, Inc., Stillwater

Pennsylvania

Carnegie Mellon University, Data Storage Systems Center, Pittsburgh
Carnegie Mellon University, Learning Systems Architecture Lab, Pittsburgh
CDG Technology, Bethlehem
ChemImage, Pittsburgh
Concurrent Technologies Corporation, Johnstown
Drexel University, Data Fusion Laboratory, Philadelphia
DRS Laurel Technologies, Johnstown
High Performance Materials Group, LLC, Boothwyn
National Institute for Occupational Safety and Health, National Personal Protective Technology Laboratory, Pittsburgh
Optical Systems Technology, Inc., Freeport
Pennsylvania State University, University Park
Saint Joseph's University, Early Responders Distance Learning Center, Philadelphia
University of Pittsburgh

Rhode Island

University of Rhode Island at Kingston

Tennessee

Atmospheric Glow Technologies, Knoxville
BWXT Y-12, Oak Ridge
Oak Ridge National Laboratory, Oak Ridge
Remotec, Inc., Oak Ridge
Turtle Mountain Communications, Inc., Maryville

Texas

Applied Research Associates, Inc., San Antonio
AptaMed, Inc., Galveston
BAE Systems, Austin
International Personnel Protection, Austin
Litton Systems, Inc., EOS Division, Garland

Lynntech, Inc., College Station
Raytheon–Advanced Systems, Plano
Southwest Research Institute, San Antonio
University of Houston
University of Texas at Austin
University of Texas at Dallas, Richardson

Utah

AccessData Corporation, Provo
Battelle Memorial Institute, Dugway
IsoForensics, Inc., Salt Lake City
University of Utah, Salt Lake City
Utah State University, Logan

Virginia

ANSER, Arlington
Applied Marine Technology, Inc., Virginia Beach
Avir, LLC, Charlottesville
Battelle Memorial Institute, Arlington
DCS Corporation, Alexandria
Defense Group, Inc., Alexandria
DTI Associates, Inc., Arlington
Dynamic Animation Systems, Fairfax
Fairfax Fire Department, Fairfax
General Dynamics Advanced Information Systems, Charlottesville
General Dynamics Network Systems, Arlington
General Testing Laboratories, Colonial Beach
Homeland Water Security Technologies, Inc., Arlington
Innovative Technology Application, Inc., Springfield
Institute for Physical Sciences, McLean
Intelligence Data Systems, Reston
International Association of Firechiefs, Fairfax
K&M Environmental, Inc., Virginia Beach
Old Dominion University, Norfolk
QinetiQ, Inc., Arlington
RASco, Inc., Woodbridge
Science Applications International Corporation, McLean
SET Associates, Arlington
Sparta, Inc., Arlington
System Planning Corporation, Arlington
The Analysis Corporation, Fairfax
The Institute for Applied Science, Reston
Titan Corporation, Reston
U.S. Naval Surface Warfare Center, Dahlgren
University of Virginia, Charlottesville
Vertex Solutions, Falls Church

Washington

Advanced Interactive Systems, Inc., Seattle
Cascade Designs, Inc., Seattle
Isotron Corporation, Seattle

MesoSystems Technology, Inc., Kennewick
Pacific Northwest National Laboratory, Richland
Washington State University at Pullman

West Virginia

MD BioTech, Morgantown
West Virginia High Technology Consortium Foundation, Fairmont
West Virginia University, Morgantown

Wisconsin

Kohler, Inc., Kohler

Wyoming

Aristatek, Inc., Laramie

International

Australia

QR Sciences, Ltd., Perth, Western Australia

Canada

Bosik, Ottawa, Ontario
British Columbia Institute of Technology, Burnaby, British Columbia
Defence Research and Development Canada, Valcartier, Quebec
Defence Research Establishment, Suffield
EOD Performance, Inc., Ottawa, Ontario
INFOSAT Telecommunication, Montreal, Quebec
Med-Eng Systems, Inc., Ottawa, Ontario
Natural Resources Canada, Canadian Explosives Research Laboratory, Ottawa, Ontario

France

University of Rennes, Brittany

Israel

Atlas Researches, Ltd., Hod Hasharon
Israel Institute for Biological Research
Israel Police National HQ, Jerusalem
Ministry of Defense, Tel Aviv
National Information Security Agency, Tel Aviv

United Kingdom

Defence Science and Technology Laboratories, Fort Halstead, Kent
Forensic Science Service, Birmingham, West Midlands
Forensic Science Service, London
Hazard Management Solutions, Ltd., Faringdon, Oxfordshire
Home Office, Police Scientific Development Branch, Sandridge, Hertfordshire
QinetiQ, Ltd., Farnborough, Hampshire
QinetiQ, Ltd., Malvern, Worcestershire
The University of Sheffield, Department of Forensic Pathology, Sheffield, South Yorkshire
TRL Technology, Ltd., Tewkesbury, Gloucestershire

A

ACC	Air Combat Command
ADL	Advanced Distributed Learning
AFIP	Armed Forces Institute of Pathology
AFRL	Air Force Research Lab
AGA	American Gas Association
AGT	Atmospheric Glow Technologies
ALON	Aluminum-Oxynitride
AMRIID	Army Medical Research Institute of Infectious Diseases
AMU	Atomic Mass Unit
ANSI	American National Standards Institute
APD	Atmospheric Plasma Decontamination
APHIS	Animal and Plant Health Inspection Service
APV	Armored Passenger Vehicle
ARIS	Advanced Radioisotope Identification System
ARS	Agricultural Research Service
ASD (SO/LIC)	Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict
ATF	Bureau of Alcohol, Tobacco, Firearms, and Explosives

B

BAA	Broad Agency Announcement
BAMS	Bio-Aerosol Mass Spectrometry
BATS	Bomb and Arson Tracking System
BIDS	BAA Information Delivery System
BTS	Border and Transportation Security

C

C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
CATS	Consequence Assessment Tool Set
CB	Chemical and/or Biological
CBIRF	Chemical Biological Incident Response Force
CBP	Customs and Border Protection
CBR	Chemical, Biological, and Radiological
CBRN	Chemical, Biological, Radiological, and Nuclear
CBRNC	Chemical, Biological, Radiological, and Nuclear Countermeasures
CBRNE	Chemical, Biological, Radiological, Nuclear, and Explosive
CDC	Centers for Disease Control and Prevention
CE	U.S. Army Corps of Engineers
CENTCOM	U.S. Central Command
CID	Criminal Investigation Command (U.S. Army)
CID	Criminal Investigation Division (EPA)
CIP	Critical Infrastructure Protection
CJTF	Combined Joint Task Force
CMLS	Chemical School
CoBRA	Chemical Biological Response Aide
CTTS	Combating Terrorism Technology Support
CTTSO	Combating Terrorism Technology Support Office

D

DARPA	Defense Advanced Research Projects Agency
DCFL	Defense Computer Forensics Laboratory
DEA	Drug Enforcement Administration
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DiCAST	Distributed Chemical Agent Sensing and Transmission
DoD	Department of Defense
DoDPI	Department of Defense Polygraph Institute
DOE	Department of Energy
DOS	Department of State
DPS	Defense Protective Service
DS	Bureau of Diplomatic Security
DTRA	Defense Threat Reduction Agency

E

ECBC	Edgewood Chemical Biological Center
ED	Explosives Detection
EDS	Electrostatic Decontamination System
EOD	Explosive Ordnance Disposal
EPA	Environmental Protection Agency
EPR	Emergency Preparedness and Response
ESC	Electronic Systems Center
EUCOM	European Command

F

FAA	Federal Aviation Administration
FAMS	Federal Air Marshal Service
FBI	Federal Bureau of Investigation
FBOP	Federal Bureau of Prisons
FDA	Food and Drug Administration
FDL	Forensic Document Laboratory
FEMA	Federal Emergency Management Agency
FLETC	Federal Law Enforcement Training Center
FORSCOM	Forces Command
FPBL	Force Protection Battle Lab
FPS	Federal Protective Service
FRA	Federal Railroad Administration
FRAT	First Responder Automated Data Tool
FS	Forest Service
FSIS	Food Safety and Inspection Service
FTA	Federal Transit Authority
FY	Fiscal Year

G

GPS	Global Positioning System
GWOT	Global War on Terrorism

H

HAZUS	Natural Hazard Loss Estimation Methodology
HHS	High Hard Steel
HMMWV	High-Mobility Multipurpose Wheeled Vehicle
HRT	Hostage Rescue Team
HSARPA	Homeland Security Advanced Research Projects Agency
HUMINT	Human Intelligence

I

IAB	InterAgency Board for Equipment Standardization and InterOperability
IAIP	Information Analysis and Infrastructure Protection
IC	Intelligence Community
ICPO	International Criminal Police Organization
ICWater	Incident Commanders Water Modeling Tool
IDD	Improvised Device Defeat
IED	Improvised Explosive Device
IG/T	Interdepartmental Working Group on Terrorism
IP	Infrastructure Protection
ISF	Investigative Support and Forensics
IWG/CT	Interagency Working Group on Counterterrorism

J

JCS	Joint Chiefs of Staff
JFCOM	Joint Forces Command
JPO-STC	Joint Program Office-Special Technology Countermeasures

L

LDV	Laser Doppler Vibrometry
LEO	Law Enforcement Online

M

M&LS	Maritime and Land Security
MANSCEN	Maneuver Support Center
MASINT	Measurement and Signature Intelligence

N

NATO	North Atlantic Treaty Organization
NAVCENT	Naval Forces Central Command
NAVEODTECHDIV	Naval Explosive Ordnance Disposal Technology Division
NAWC	Naval Air Warfare Center
NCFS	National Center for Forensic Science
NCIS	Naval Criminal Investigative Service
NEIC	National Enforcement Investigations Center
NFPA	National Fire Protection Association
NFSTC	National Forensic Science Technology Center
NGB	National Guard Bureau
NGIC	National Ground Intelligence Center
NHTSA	National Highway Traffic Safety Administration
NIJ	National Institute of Justice
NIOSH	National Institute for Occupational Safety and Health

NIPC	National Infrastructure Protection Center
NIST	National Institute of Standards and Technology
NNSA	National Nuclear Security Administration
NRL	Naval Research Laboratory
NRO	National Reconnaissance Office
NSA	National Security Agency
NSWC	Naval Surface Warfare Center

O

OATSD/CBD	Office of the Assistant to the Secretary of Defense for Chemical and Biological Defense
OBO	Overseas Building Operations
ODP	Office for Domestic Preparedness
OEA	Office of Energy Assurance
OIF	Operation Iraqi Freedom
OIS	Office of Information Services
OJP	Office of Justice Programs
OLES	Office of Law Enforcement Standards
OS	Office of Security
OSI	Office of Special Investigations
OUSD/AT&L	Office of the Under Secretary of Defense for Acquisition, Technology,and Logistics
OUSD/PR	Office of the Under Secretary of Defense for Personnel and Readiness

P

PAN	Percussion Actuated Non-electric
PDA	Personal Digital Assistant
PFPA	Pentagon Force Protection Agency
PNNL	Pacific Northwest National Laboratory
PPE	Personal Protective Equipment
PS	Physical Security
PSG	Personnel Screening Guide

Q

QR	Quadrupole Resonance

R

R&D	Research and Development
RD&E	Research, Development, and Engineering
RFD	Remote Firing Device
RHA	Rolled Homogeneous Armor
RIG	Railcar Inspection Guide
RNA	Ribonucleic Acid
RTR	Real-Time Radiographic

S

S/CT	Department of State, Office of the Coordinator for Counterterrorism
S&T	Science and Technology
SAA	Sergeant at Arms
SBCCOM	Soldier and Biological Chemical Command

SCADA	Supervisory Control and Data Acquisition
SCCU	Stand-Off Connectivity Control Unit
SCOS	Surveillance, Collection, and Operations Support
SG	Surgeon General
SO/LIC	Special Operations and Low-Intensity Conflict
SOCOM	Special Operations Command
SOP	Standard Operating Procedure
SSD	Special Services Division
SWC	Special Warfare Center
SWIG	Small Watercraft Inspection Guide
SWIP	Sensor Web for Infrastructure Protection

T

TACOM	Tank-Automotive and Armaments Command
TB	Tuberculosis
TEU	Technical Escort Unit
TOS	Tactical Operations Support
TSA	Transportation Security Administration
TSD	Technical Security Division
TSP	Training Support Package
TSWG	Technical Support Working Group
TTD	Training Technology Development
TTFD	Tactical Timed Firing Device
TTL	Tagging, Tracking, and Locating

U

USA	United States Army
USAF	United States Air Force
USAR	United States Army Reserve
USCG	United States Coast Guard
USFA	United States Fire Administration
USMC	United States Marine Corps
USMS	United States Marshals Service
USN	United States Navy
USNAVEUR	United States Naval Forces Europe
USPIS	United States Postal Inspection Service
USSS	United States Secret Service

V

VBIED	Vehicle-Borne Improvised Explosive Device
VIC	Vehicle Inspection Checklist
VIP	Very Important Person
VIPS	Vessel Identification and Positioning System
VPAT	Virus Propagation Analysis Tool
VSP	Visual Sample Plan

W

WMD	Weapon of Mass Destruction

Combating Terrorism Technology Support Office